

From the INTERNATIONAL BUREAU

**PCT****NOTIFICATION OF ELECTION**

(PCT Rule 61.2)

To:

Commissioner  
US Department of Commerce  
United States Patent and Trademark  
Office, PCT  
2011 South Clark Place Room  
CP2/5C24  
Arlington, VA 22202  
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

<b>Date of mailing</b> (day/month/year) 02 May 2001 (02.05.01)	
<b>International application No.</b> PCT/JP00/05832	<b>Applicant's or agent's file reference</b> 900392
<b>International filing date</b> (day/month/year) 29 August 2000 (29.08.00)	<b>Priority date</b> (day/month/year) 30 August 1999 (30.08.99)
<b>Applicant</b> HATANAKA, Masayuki et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:

26 March 2001 (26.03.01)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

<b>The International Bureau of WIPO</b> 34, chemin des Colombettes 1211 Geneva 20, Switzerland	<b>Authorized officer</b> Kiwa Mpay
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

1

This Page Blank (uspto)

# PATENT COOPERATION TREATY

**PCT**

From the INTERNATIONAL BUREAU

## NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and  
Administrative Instructions, Section 422)

To:

FUKAMI, Hisao  
Mitsui Sumitomo Bank  
Minamimorimachi Bldg.  
1-29, Minamimorimachi 2-chome,  
Kita-ku  
Osaka-shi, Osaka 530-0054  
JAPON

<b>Date of mailing (day/month/year)</b> 17 July 2001 (17.07.01)	
<b>Applicant's or agent's file reference</b> 900392	<b>IMPORTANT NOTIFICATION</b>
<b>International application No.</b> PCT/JP00/05832	<b>International filing date (day/month/year)</b> 29 August 2000 (29.08.00)

1. The following indications appeared on record concerning:

☐ the applicant
 ☐ the inventor
 ☒ the agent
 ☐ the common representative

Name and Address

1) FUKAMI, Hisao  
 2) MORITA, Toshio  
 3) HORII, Yutaka  
 Sumitomo Bank Minamimori-machi Building  
 1-29, Minamimori-machi 2-chome  
 Kita-ku, Osaka-shi  
 Osaka 530-0054  
 Japan

State of Nationality

State of Residence

Telephone No.

06-6361-2021

Facsimile No.

06-6361-1731

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person
 ☐ the name
 ☒ the address
 ☐ the nationality
 ☐ the residence

Name and Address

1) FUKAMI, Hisao  
 2) MORITA, Toshio  
 3) HORII, Yutaka  
 Mitsui Sumitomo Bank Minamimorimachi Bldg.  
 1-29, Minamimorimachi 2-chome,  
 Kita-ku, Osaka-shi, Osaka 530-0054  
 Japan

State of Nationality

State of Residence

Telephone No.

06-6361-2021

Facsimile No.

06-6361-1731

Teleprinter No.

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

<input checked="" type="checkbox"/> the receiving Office	<input type="checkbox"/> the designated Offices concerned
<input checked="" type="checkbox"/> the International Searching Authority	<input checked="" type="checkbox"/> the elected Offices concerned
<input type="checkbox"/> the International Preliminary Examining Authority	<input type="checkbox"/> other:

The International Bureau of WIPO  
 34, chemin des Colombettes  
 1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Shinji IGARASHI

Telephone No.: (41-22) 338.83.38

**This Page Blank (uspto)**

10T  
Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 900392	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/JP00/05832	International filing date (day month year) 29 August 2000 (29.08.00)	Priority date (day month year) 30 August 1999 (30.08.99)
International Patent Classification (IPC) or national classification and IPC G10K 15/02, G06F 15/00, 17/60, H04L 9/08, 9/10, G06K 19/00, H04H 1/00, H04M 3/42, 3/493, 11/08, G10L 19/00		
Applicant FUJITSU LIMITED		

- This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
- This REPORT consists of a total of 5 sheets, including this cover sheet.  
☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 19 sheets.

- This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 26 March 2001 (26.03.01)	Date of completion of this report 17 September 2001 (17.09.2001)
Name and mailing address of the IPEA/JP	Authorized officer
Facsimile No.	Telephone No.

**This Page Blank (uspto)**

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/JP00/05832

## I. Basis of the report

1. With regard to the **elements** of the international application:\*

- ☐ the international application as originally filed
- ☒ the description:  
pages 4-35, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages 1-3.3/1-3/4, filed with the letter of 20 June 2001 (20.06.2001)
- ☒ the claims:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, as amended (together with any statement under Article 19  
pages \_\_\_\_\_, filed with the demand  
pages 1-14, filed with the letter of 20 June 2001 (20.06.2001)
- ☒ the drawings:  
pages 1-22, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_
- ☐ the sequence listing part of the description:  
pages \_\_\_\_\_, as originally filed  
pages \_\_\_\_\_, filed with the demand  
pages \_\_\_\_\_, filed with the letter of \_\_\_\_\_

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language \_\_\_\_\_ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/fig \_\_\_\_\_

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).\*\*

\* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

\*\* Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

This Page Blank (uspto)



**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement****1. Statement**

Novelty (N)	Claims	1-41	YES
	Claims		NO
Inventive step (IS)	Claims	1-41	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-41	YES
	Claims		NO

**2. Citations and explanations**

## Claims 1-5

Document 1 (EP, 817185, A2 (Toshiba Corp.), 7 January 1998 (07.01.98)) and Document 2 ("Kogata memori kaado de ongaku chosakuken wo mamoru" [Protecting musical copyright with small memory cards], Nikkei Electronics, No. 739, 22 March 1999 (22.03.99), pp. 49-53) are documents defining the general state of the art in the technical field in question, disclosing data reproduction devices using a plurality of keys. However, none of the documents cited in the international search report or documents newly cited in the international preliminary examination report discloses or suggests the feature of a data storage component which stores a content key encrypted in a code which can be decrypted by a specific key in the data reproduction component.

## Claims 6-11

Documents 1 and 2 are documents defining the general state of the art in the technical field in question, disclosing data reproduction devices using a plurality of keys. However, none of the documents cited in the international search report or documents newly cited in the international preliminary examination report discloses or suggests the feature of a data storage component which

This Page Blank (uspto)

encrypts a session key which is different for each access to obtain the content keys, using a code that can be decrypted by a specific key in the data reproduction component, and feeds this to the data reproduction component.

Claims 12-22 and 31-41

Documents 1 and 2 are documents defining the general state of the art in the technical field in question, disclosing data reproduction devices using a plurality of keys. However, none of the documents cited in the international search report or documents newly cited in the international preliminary examination report discloses or suggests the feature of a data storage component which encrypts session key which is different for each access to obtain content data, using a code that can be decrypted by a specific key in the data reproduction component, and feeds this to the data reproduction component.

Claims 23-30

Documents 1 and 2 are documents defining the general state of the art in the technical field in question, disclosing data reproduction devices using a plurality of keys. However, none of the documents cited in the international search report or documents newly cited in the international preliminary examination report discloses or suggests the feature of a data reproduction module using a specific key for the data reproduction component and a session key encoded by a separate session key.

This Page Blank (uspto)

**VII. Certain defects in the international application**

The following defects in the form or contents of the international application have been noted:

In the description, page 36, line 12, the "session key generating component" is given the number "1520", but in Fig. 4, number "1520" is the "decrypting treatment component" and not the "session key generating component". Therefore, the number is not used consistently throughout the whole of the international application.

Similarly, in the description, page 36, lines 14-15, the "first encryption treatment component" is given the number "1540", but in Fig. 4, number "1540" is the "Kp holding component" and not the "first encryption treatment component". Therefore, the number is not used consistently throughout the whole of the international application.

This Page Blank (uspto)

## 国際調査報告

(法8条、法施行規則第40、41条)  
[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号	900392	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。	
国際出願番号 PCT/JP00/05832	国際出願日 (日.月.年)	29.08.00	優先日 (日.月.年) 30.08.99
出願人(氏名又は名称) 富士通株式会社			

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。  
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

## 1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☐ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 2 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

This Page Blank (uspto)



## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int Cl<sup>1</sup> G10K15/02, G06F15/00, G06F17/60, H04L9/08, H04L9/10,  
G06K19/00, H04H1/00, H04M3/42, H04M3/493, H04M11/08,  
G10L19/00

## B. 調査を行った分野

## 調査を行った最小限資料 (国際特許分類 (IPC))

Int Cl<sup>1</sup> G10K15/00~15/06, G10L19/00~19/14, H04L9/00~9/38,  
G09C1/00~5/00, G06F12/00, G06F12/14, H04M11/00~11/10

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926~1995年  
日本国公開実用新案公報 1971~2000年  
日本国登録実用新案公報 1994~2000年  
日本国実用新案登録公報 1996~2000年

## 国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

INSPEC (DIALOG)  
WPI (DIALOG)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	EP, 817185, A2 (Kabushiki kaisha TOSHIBA) 7.1月.1998(07.01.98), 全文全図, &JP, 10-106148, A &JP, 3093678, B2 &TW, 340920, A &KR, 98086354, A &CN, 1183685, A	1
Y		2-22
X	JP, 9-326166, A (三菱電機株式会社) 16.12月.1997(16.12.97), 全文全図, (ファミリーなし)	1
Y		2-22

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

10.11.00

国際調査報告の発送日

21.11.00

国際調査機関の名称及び先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

松尾 淳一

印

5C

8842

電話番号 03-3581-1101 内線 3540

**This Page Blank (uspto)**

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 10-40172, A (株式会社東芝) 13.2月.1998(13.2.98), 全文全図, (ファミリーなし)	2-22
Y	日経エレクトロニクス, No.739, 「小型メモリ・カードで音楽著作権を守る」, 22.3月.1999(22.03.99), p.49-53	2-22
Y	日経エレクトロニクス, No.728, 「米周辺機器メーカー大手が, MP3携帯型プレーヤ発売 著作権対策は付加せず」, 19.10月.1998(19.10.98), p.31-32	2-22
A	日経エレクトロニクス, No.731, 「汚れたイメージ払拭ねらうMP3業界 音楽配信の会議 Webnoise から」, 30.11月.1998(30.11.98), p.29-30	1-22

**This Page Blank (uspto)**

PCT

国際予備審査報告

(法第12条、法施行規則第56条)  
[PCT36条及びPCT規則70]

REC'D 28 SEP 2001

WIPO

PCT

出願人又は代理人 の書類記号	900392	今後の手続きについては、国際予備審査報告の送付通知（様式PCT/ IPEA/416）を参照すること。	
国際出願番号 PCT/JPO0/05832	国際出願日 (日.月.年) 29.08.00	優先日 (日.月.年) 30.08.99	
国際特許分類 (IPC)	Int Cl <sup>7</sup> G10K15/02, G06F15/00, G06F17/60, H04L9/08, H04L9/10, G06K19/00, H04H1/00, H04M3/42, H04M3/493, H04M11/08, G10L19/00		
出願人 (氏名又は名称)	富士通株式会社		

- 国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条 (PCT36条) の規定に従い送付する。
- この国際予備審査報告は、この表紙を含めて全部で 4 ページからなる。  
☒ この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び/又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び/又は図面も添付されている。  
(PCT規則70.16及びPCT実施細則第607号参照)  
この附属書類は、全部で 19 ページである。

- この国際予備審査報告は、次の内容を含む。
  - ☒ 国際予備審査報告の基礎
  - ☐ 優先権
  - ☐ 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
  - ☐ 発明の単一性の欠如
  - ☒ PCT35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
  - ☐ ある種の引用文献
  - ☒ 国際出願の不備
  - ☐ 国際出願に対する意見

国際予備審査の請求書を受理した日 26.03.01	国際予備審査報告を作成した日 17.09.01	
名称及びあて先 日本国特許庁 (IPEA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 榎本 剛	5C 9379
	電話番号 03-3581-1101 内線 3541	

This Page Blank (uspto)

## I. 国際予備審査報告の基礎

1. この国際予備審査報告は下記の出願書類に基づいて作成された。(法第6条(PCT14条)の規定に基づく命令に  
応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。  
PCT規則70.16, 70.17)

☐ 出願時の国際出願書類

☒ 明細書 第 4 - 35 ページ、 出願時に提出されたもの  
明細書 第 ページ、 国際予備審査の請求書と共に提出されたもの  
明細書 第 1 - 3, 3/1- 3/4 ページ、 20.06.01 付の書簡と共に提出されたもの

☒ 請求の範囲 第 項、 出願時に提出されたもの  
請求の範囲 第 項、 PCT19条の規定に基づき補正されたもの  
請求の範囲 第 項、 国際予備審査の請求書と共に提出されたもの  
請求の範囲 第 1 - 41 項、 20.06.01 付の書簡と共に提出されたもの

☒ 図面 第 1 - 22 ページ/図、 出願時に提出されたもの  
図面 第 ページ/図、 国際予備審査の請求書と共に提出されたもの  
図面 第 ページ/図、 付の書簡と共に提出されたもの

☐ 明細書の配列表の部分 第 ページ、 出願時に提出されたもの  
明細書の配列表の部分 第 ページ、 国際予備審査の請求書と共に提出されたもの  
明細書の配列表の部分 第 ページ、 付の書簡と共に提出されたもの

2. 上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である 語である。

- ☐ 国際調査のために提出されたPCT規則23.1(b)にいう翻訳文の言語  
☐ PCT規則48.3(b)にいう国際公開の言語  
☐ 国際予備審査のために提出されたPCT規則55.2または55.3にいう翻訳文の言語

3. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

- ☐ この国際出願に含まれる書面による配列表  
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表  
☐ 出願後に、この国際予備審査(または調査)機関に提出された書面による配列表  
☐ 出願後に、この国際予備審査(または調査)機関に提出されたフレキシブルディスクによる配列表  
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった  
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

4. 補正により、下記の書類が削除された。

☐ 明細書 第 ページ  
☐ 請求の範囲 第 項  
☐ 図面 図面の第 ページ/図

5. ☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。(PCT規則70.2(c) この補正を含む差し替え用紙は上記1.における判断の際に考慮しなければならず、本報告に添付する。)

This Page Blank (uspto)



## V. 新規性、進歩性又は産業上の利用可能性についての法第12条(PCT35条(2))に定める見解、それを裏付ける文献及び説明

## 1. 見解

新規性 (N)	請求の範囲	1-41	有
	請求の範囲		無
進歩性 (IS)	請求の範囲	1-41	有
	請求の範囲		無
産業上の利用可能性 (IA)	請求の範囲	1-41	有
	請求の範囲		無

## 2. 文献及び説明 (PCT規則70.7)

## 請求項1-5

文献1: EP 817185 A2 (Kabushiki kaisha TOSHIBA) 7.1月.1998  
(07.01.98)

および

文献2: 日経エレクトロニクス, No. 739, 「小型メモリ・カードで音楽著作権を守る」, 22.3月.1999(22.03.99), p. 49-53

には、当該技術分野の一般的技術水準を示す文献として、複数の鍵を用いたデータ再生装置が記載されているが、データ再生部に固有な鍵にて復号可能な暗号を施された暗号化コンテンツキーをデータ格納部に格納する技術に関しては、国際調査報告にて列記した文献、および国際予備審査報告にて新たに引用した文献のいずれにも、記載も示唆もされていない。

## 請求項6-11

文献1および文献2には、当該技術分野の一般的技術水準を示す文献として、複数の鍵を用いたデータ再生装置が記載されているが、コンテンツキーの取得のためのアクセスごとに異なるセッションキーをデータ再生部に固有な鍵により復号可能な暗号化を施して、データ再生部に供給するデータ格納部の技術に関しては、国際調査報告にて列記した文献、および国際予備審査報告にて新たに引用した文献のいずれにも、記載も示唆もされていない。

## 請求項12-22, 31-41

文献1および文献2には、当該技術分野の一般的技術水準を示す文献として、複数の鍵を用いたデータ再生装置が記載されているが、コンテンツデータの取得のためのアクセスごとに異なるセッションキーをデータ再生部に固有な鍵により復号可能な暗号化を施して、データ再生部に供給するデータ格納部の技術に関しては、国際調査報告にて列記した文献、および国際予備審査報告にて新たに引用した文献のいずれにも、記載も示唆もされていない。

## 請求項23-30

文献1および文献2には、当該技術分野の一般的技術水準を示す文献として、複数の鍵を用いたデータ再生装置が記載されているが、データ再生部に固有な鍵および別のセッションキーにより暗号化を施されたセッションキーを用いたデータ再生モジュールの技術に関しては、国際調査報告にて列記した文献、および国際予備審査報告にて新たに引用した文献のいずれにも、記載も示唆もされていない。

This Page Blank (uspto)

## VII. 国際出願の不備

この国際出願の形式又は内容について、次の不備を発見した。

明細書第36頁第12行に記載された「セッションキー発生部」には「1520」の記号が付されているが、第4図の符号「1520」の部分は「セッションキー発生部」ではなく「復号処理部」である。したがって、記号が国際出願の全体を通じて一貫して使用されていない。

また、明細書第36頁第14～15行に記載された「第1の暗号化処理部」には「1540」の記号が付されているが、第4図の符号「1540」の部分は「第1の暗号化処理部」ではなく「Kp保持部」である。したがって、記号が国際出願の全体を通じて一貫して使用されていない。

This Page Blank (uspto)

## 明細書

## データ再生装置およびデータ再生モジュール

## 5 技術分野

本発明は、携帯電話網等のデータ配信システムにより配送された配信データの再生装置に関し、より特定のには、配信されたデータに対する著作権保護を可能とするデータ再生装置に関するものである。

## 10 背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽データや画像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

したがって、このような情報通信網上において、音楽データや画像データ等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ところで、上述したようなデジタル情報通信網を介した音楽データなどの著作権データの配信が行なわれた場合、各ユーザは、このようにして配信されたデータを何らかの記録装置に記録した上で、再生装置で再生することになる。

このような記録装置としては、たとえば、メモ리카ードのように電氣的にデー

*This Page Blank (uspto)*

タの書込および消去が可能な媒体が用いられることになる。

さらに、配信データを再生する装置としては、このようなデータの配信を受けるのに用いた携帯電話機自身を用いる場合や、あるいは、記録装置がメモリーカードなどのように配信を受ける装置から着脱可能な場合は、専用の再生装置を用いることも可能である。

この場合、著作権者の権利保護のためには、著作権者の承諾なしに、このようにして配信を受けたコンテンツデータ（音楽データ等）を自由に当該記録媒体から他の記録媒体等へ移転できないように記録媒体においてセキュリティ対策を施す必要がある。

そのみならず、このようにして正当な対価を支払った上でコンテンツデータの配信を受けたユーザ以外のものが、当該記録媒体から音楽データ等の再生を行なう際に、再生装置側においてコンテンツデータを外部から自由に読み出すことができる」とすると、著作権者の権利保護ならびに正規のユーザ側の権利保護にも支障を来すことになる。

#### 発明の開示

本発明の目的は、配信されて記録装置に保持された音楽データ等の著作物データを再生する再生装置において、ユーザ以外の者が無断で当該著作物データに対してアクセスを行なうことから保護する機能を備えたデータ再生装置を提供することである。

係る目的を達成するために本願発明に係るデータ再生装置は、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、データ再生部と、データ格納部とを備える。

データ再生部は、暗号化コンテンツデータを再生する。データ格納部は、暗号化コンテンツデータと暗号化コンテンツデータを復号するためのコンテンツキーをデータ再生部に固有な第1の復号鍵にて復号可能な暗号を施された暗号化コンテンツキーとを格納し、かつデータ再生部に出力する。

データ再生部は、セッションキー発生部と、第1の暗号化処理部と、第1の復号処理部と、第1の鍵保持部と、第2の復号処理部と、第3の復号処理部とを含む。

***This Page Blank (uspto)***



む。

セッションキー発生部は、データ格納部に対してコンテンツキーの取得のためにアクセスするごとに更新されるセッションキーを生成する。第1の暗号化処理部は、セッションキーをデータ格納部にて復号可能で、かつデータ格納部に固有な公開暗号鍵で暗号化してデータ格納部に与える。第1の復号処理部は、セッションキーで暗号化された上でデータ格納部から取得した暗号化コンテンツキーを、セッションキーを用いて復号する。

第1の鍵保持部は、第1の復号鍵を予め保持する。第2の復号処理部は、第1の鍵保持部に保持される第1の復号鍵を用いて第1の復号処理部からの出力に対して復号処理を行なうことで、コンテンツキーを抽出する。第3の復号処理部は、データ格納部から読出された暗号化コンテンツデータを受けて、第2の復号処理部にて抽出されたコンテンツキーを用いて復号してコンテンツデータを抽出する。

この発明の他の局面に従うと、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、データ再生部と、データ格納部とを備える。

データ再生部は、暗号化コンテンツデータを暗号化コンテンツデータを復号するためのコンテンツキーを用いて復号してコンテンツデータを再生する。データ格納部は、暗号化コンテンツデータおよびコンテンツキーを格納し、コンテンツキーの取得のためにアクセスされるごとに異なる第1のセッションキーをデータ再生部に固有な固有復号鍵により復号可能な暗号化を施して、データ再生部に供給する。

データ再生部は、第1の鍵保持部と、第1の復号処理部と、第1のセッションキー発生部と、第1の暗号化処理部と、第2の復号処理部と、第3の復号処理部を含む。

第1の鍵保持部は、固有復号鍵を予め保持する。第1の復号処理部は、第1の鍵保持部からの出力である固有復号鍵を用いて復号処理を行なう。第1のセッションキー発生部は、データ格納部に対してコンテンツキーの取得のためにアクセスするごとに更新される第2のセッションキーを生成する。第1の暗号化処理部は、データ格納部から供給された固有復号鍵にて復号可能な暗号化を施された第1の

**This Page Blank (uspto)**

セッションキーを第1の復号処理部にて復号し、復号された第1のセッションキーにより、第2のセッションキーを暗号化してデータ格納部に与える。第2の復号処理部は、固有復号鍵にて復号可能な暗号化を施され、かつ、第2のセッションキーで暗号化された上でデータ格納部から供給されたコンテンツキーを、第2のセッションキーについて復号する。第1の復号処理部は、固有復号鍵を用いて第2の復号処理部からの出力に対してさらに復号処理を行なうことで、コンテンツキーを抽出する。第3の復号処理部は、データ格納部から供給された暗号化コンテンツデータを受けて、第1の復号処理部により抽出されたコンテンツキーにより復号して、コンテンツデータを抽出する。

10 この発明のさらに他の局面に従うと、暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、データ再生部と、データ格納部とを備える。

データ再生部は、暗号化コンテンツデータを暗号化コンテンツデータを復号するためのコンテンツキーを用いて復号して、コンテンツデータを再生する。データ格納部は、暗号化コンテンツデータおよびコンテンツキーを格納し、かつ、暗号化コンテンツデータの取得のためのアクセスされるごとに異なる第1のセッションキーをデータ再生部に固有な固有復号鍵により復号可能な暗号化を施してデータ再生部に供給する。

データ再生部は、鍵保持部と、第1の復号処理部と、セッションキー発生部と、第1の暗号化処理部と、第2の復号処理部と、第3の復号処理部とを備える。

鍵保持部は、固有復号鍵を予め保持する。第1の復号処理部は、データ格納部から供給された固有復号鍵にて復号可能な暗号化を施された第1のセッションキーを、固有復号鍵にて復号して抽出する。セッションキー発生部は、データ格納部に対してコンテンツキーの取得のためにアクセスするごとに更新される第2のセッションキーを生成する。第1の暗号化処理部は、第2のセッションキーを第1のセッションキーで暗号化してデータ格納部に与える。第2の復号処理部は、第2のセッションキーで暗号化されてデータ格納部から供給されたコンテンツキーを、第2のセッションキーについて復号する。第3の復号処理部は、データ格納部から供給された暗号化コンテンツデータを受けて、第2の復号処理部の出力

***This Page Blank (uspto)***

に基づいて復号してコンテンツデータを抽出する。

この発明のさらに他の局面に従うと、暗号化コンテンツデータを復号してコンテンツデータを再生するためのデータ再生装置に搭載するデータ再生モジュールであって、第1の鍵保持部と、第1の復号処理部と、セッションキー発生部と、  
5 暗号化処理部と、第2の復号処理部と、第3の復号処理部とを備える。

第1の鍵保持部は、データ再生モジュールに固有な第1の復号鍵を予め保持する。第1の復号処理部は、暗号化コンテンツデータを復号するための復号鍵であるコンテンツキーの取得のためのアクセスごとに第2の復号鍵により復号可能な暗号化処理を施されてデータ再生モジュールの外部から供給される第1のセッションキーを、第1の復号鍵にて復号して抽出する。セッションキー発生部は、データ再生モジュールの外部に対してコンテンツキーの取得のためにアクセスするごとに更新される第2のセッションキーを生成する。暗号化処理部は、第2のセッションキーを第1のセッションキーを用いて暗号化してデータ再生モジュールの外部に与える。第2の復号処理部は、第2のセッションキーで暗号化されてデータ再生モジュールの外部から供給されるコンテンツキーを、第2のセッションキーを用いて復号する。第3の復号処理部は、データ再生モジュールの外部から供給される暗号化コンテンツデータを受けて、第2の復号処理部の出力に基づいて復号してコンテンツデータを抽出する。  
10  
15

この発明のさらに他の局面に従うと、暗号化コンテンツデータおよび暗号化コンテンツデータを復号してコンテンツデータを得るための復号鍵であるコンテンツキーを格納し、かつ暗号化コンテンツデータの取得のためにアクセスされるごとに異なる第1のセッションキーをデータ再生装置に固有な固有復号鍵により復号可能な暗号化を施してデータ再生装置に供給するデータ記録部を装着して、データ記録装置に格納された暗号化コンテンツデータを、データ記録装置に格納された暗号化コンテンツキーを用いて再生するためのデータ再生装置であって、第1のインターフェイスと、鍵保持部と、第1の復号処理部と、セッションキー発生部と、暗号化処理部と、第2の復号処理部と、第3の復号処理部とを備える。  
20  
25

第1のインターフェイスは、データ記録装置を装着し、かつ、データ記録装置との間でデータの授受を行なう。鍵保持部は、データ再生装置に固有な固有鍵を

***This Page Blank (uspto)***

予め保持する。第1の復号処理部は、コンテンツキーの取得のためのアクセスごとに更新され、かつデータ再生装置に固有な固有復号鍵により復号可能な暗号化を施されてデータ記録装置から供給される第1のセッションキーを、固有復号鍵にて復号して抽出する。セッションキー発生部は、データ記録装置に対する暗号化コンテンツキーの取得のためにアクセスするごとに更新される第2のセッションキーを生成する。暗号化処理部は、第2のセッションキーを第1のセッションキーを用いて暗号化してデータ記録装置に与える。第2の復号処理部は、第2のセッションキーで暗号化されてデータ記録装置から供給されるコンテンツキーを、第2のセッションキーを用いて復号する。第3の復号処理部は、データ記録装置から読出された暗号化コンテンツデータを受けて、第2の復号処理部の出力に基づいて復号してコンテンツデータを抽出する。

したがって、本願発明にかかるデータ再生装置によれば、正規のユーザがメモリ中に格納したコンテンツデータに対して、第三者が不当に配信データへのアクセスを行なうことが困難な構成となっているので、著作権者および正当なユーザが、無断で行なわれる不当な処理により不利益を被るのを防止することが可能となる。

#### 図面の簡単な説明

図1は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

図2は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

図3は、携帯電話機100内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

図4は、本発明の実施例2の携帯電話機200の構成を説明するための概略ブロック図である。

図5は、図4に示した携帯電話機200において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

図6は、図4に示したメモリカード120の構成を説明するための概略ブロッ

**This Page Blank (uspto)**



ク図である。

図 7 は、携帯電話機 200 内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

図 8 は、本発明の実施例 3 の携帯電話機 300 の構成を説明するための概略ブロック図である。

図 9 は、図 8 に示した携帯電話機 300 において使用される通信のためのキー

**This Page Blank (uspto)**

## 請求の範囲

1. (補正後) 暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置 (200) であって、

5 前記暗号化コンテンツデータを再生するためのデータ再生部 (1500) と、  
前記暗号化コンテンツデータと前記暗号化コンテンツデータを復号するためのコンテンツキーを前記データ再生部に固有な第1の復号鍵にて復号可能な暗号を施された暗号化コンテンツキーとを格納し、かつ前記データ再生部に出力するためのデータ格納部 (120) とを備え、

10 前記データ再生部は、  
前記データ格納部に対して前記コンテンツキーの取得のためにアクセスするごとに更新されるセッションキーを生成するセッションキー発生部 (1520) と、  
前記セッションキーを前記データ格納部にて復号可能で、かつ前記データ格納部に固有な公開暗号鍵で暗号化して前記データ格納部に与えるための第1の暗号  
15 化処理部 (1540) と、

前記セッションキーで暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記セッションキーを用いて復号する第1の復号処理部 (1506) と、

前記第1の復号鍵を予め保持する第1の鍵保持部 (1540) と、

20 前記第1の鍵保持部に保持される前記第1の復号鍵を用いて前記第1の復号処理部からの出力に対して復号処理を行なうことで、前記コンテンツキーを抽出する第2の復号処理部 (1530) と、

前記データ格納部から読出された前記暗号化コンテンツデータを受けて、前記第2の復号処理部にて抽出されたコンテンツキーを用いて復号してコンテンツデータを抽出するための第3の復号処理部 (1520) とを含む、データ再生装置。  
25

2. (補正後) 前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生部は、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音

***This Page Blank (uspto)***

楽再生部（1508）と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部（1512）とをさらに含む、請求項1に記載のデータ再生装置。

5 3.（補正後）前記データ再生部は、第三者には読出不可能なセキュリティ領域に設けられる、請求項1に記載のデータ再生装置。

4.（補正後）前記データ格納部（120）は、

前記データ格納部に与えられるデータを保持するための記録部（1412）と、  
前記データ格納部に固有な前記公開暗号鍵を保持し、前記データ再生部へ供給可能な第2の鍵保持部（1401）と、

10 前記公開暗号鍵により暗号化されたデータを復号するための第2復号鍵を保持する第3の鍵保持部（1402）と、

前記第2の復号鍵を用いて、前記データ再生部から前記公開暗号鍵により暗号化されて伝達された前記第1のセッションキーを復号するための第4の復号処理部（1404）と、

15 前記第4の復号処理部で抽出された前記第1のセッションキーにより、前記記録部に格納された暗号化コンテンツキーを暗号化して出力するための第2の暗号化処理部（1406）とを備える、請求項1に記載のデータ再生装置。

5.（補正後）前記データ格納部は、前記データ再生部に対して着脱可能である、請求項1に記載のデータ再生装置。

20 6.（補正後）暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置（300、400）であって、

前記暗号化コンテンツデータを前記暗号化コンテンツデータを復号するためのコンテンツキーを用いて復号してコンテンツデータを再生するためのデータ再生部（1500）と、

25 前記暗号化コンテンツデータおよび前記コンテンツキーを格納し、前記コンテンツキーの取得のためにアクセスされるごとに異なる第1のセッションキーを前記データ再生部に固有な固有復号鍵により復号可能な暗号化を施して、前記データ再生部に供給するデータ格納部（130、140）とを備え、

前記データ再生部は、

*This Page Blank (uspto)*

前記データ格納部に対して前記コンテンツキーの取得のためにアクセスするご  
に更新される第2のセッションキーを生成する第1のセッションキー発生部  
(1522)と、

前記固有復号鍵にて復号可能な暗号化を施され、かつ、前記第2のセッションキーで暗号化された上で前記データ格納部から供給された前記コンテンツキーを、前記第2のセッションキーについて復号する第2の復号処理部（1556）とを含み、

少なくとも前記第 1 の鍵保持部と、前記第 1 の復号処理部と、前記第 2 の復号

This Page Blank (uspto)



処理部と、前記第 3 の復号処理部とが、第三者には読出不可能なセキュリティ領域に設けられる、請求項 7 に記載のデータ再生装置。

9. (補正後) 前記データ格納部 (130, 140) は、

前記データ格納部に与えられるデータを格納するための記録部 (1412) と、

5 前記第 1 のセッションキーを発生する第 2 のセッションキー発生部 (1450) と、

前記データ再生部に固有でかつ前記固有復号鍵にて復号可能な暗号化を施すための公開暗号鍵により、暗号化処理を行なう第 2 の暗号化処理部 (1452) と、

10 前記第 1 のセッションキーを用いて、前記データ再生部から前記第 1 のセッションキーにて暗号化されて伝達された前記第 2 のセッションキーを復号するための第 4 の復号処理部 (1454) と、

前記第 4 の復号処理部にて抽出された前記第 1 のセッションキーにより、暗号化処理を行ない出力するための第 3 の暗号化処理部 (1456) とを備え、

15 前記記録部に格納された前記コンテンツキーを前記第 2 の暗号化処理部にて暗号化し、さらに前記第 3 の暗号化処理部にて暗号化して、前記データ再生部に供給する、請求項 6 に記載のデータ再生装置。

10. (補正後) 前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項 6 に記載のデータ再生装置。

11. (補正後) 前記データ再生装置は、

20 前記データ再生部に固有な認証データとともに前記公開暗号鍵を、前記データ格納部にて認証鍵により復号可能な暗号化を施して保持し、前記データ格納部に供給する認証データ保持部 (1560) をさらに備え、

前記データ格納部 (140) は、

25 前記認証鍵により暗号化されて前記データ再生部から与えられる前記認証データと前記公開暗号鍵を復号して抽出するための第 5 の復号処理部 (1460) と、

前記第 5 の復号処理部により抽出された前記認証データに基づいて前記認証データを出力したデータ再生部に対して前記コンテンツキーを出力するか否かを判断する認証処理を行なう制御手段 (1420) とを含む、請求項 9 に記載のデータ再生装置。

This Page Blank (uspto)

1 2. (補正後) 暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置(500, 600)であって、

前記暗号化コンテンツデータを前記暗号化コンテンツデータを復号するためのコンテンツキーを用いて復号して、コンテンツデータを再生するためのデータ再生部と、

前記暗号化コンテンツデータおよび前記コンテンツキーを格納し、かつ、前記暗号化コンテンツデータの取得のためのアクセスされるごとに異なる第1のセッションキーを前記データ再生部に固有な固有復号鍵により復号可能な暗号化を施して前記データ再生部に供給するデータ格納部(150, 160)とを備え、

前記データ再生部は、

前記固有復号鍵を予め保持する鍵保持部(1540)と、

前記データ格納部から供給された前記固有復号鍵にて復号可能な暗号化を施された前記第1のセッションキーを、前記固有復号鍵にて復号して抽出する第1の復号処理部(1530)と、

前記データ格納部に対して前記コンテンツキーの取得のためにアクセスするごとに更新される第2のセッションキーを生成するセッションキー発生部(1552)と、

前記第2のセッションキーを前記第1のセッションキーで暗号化して前記データ格納部に与えるための第1の暗号化処理部(1554)と、

前記第2のセッションキーで暗号化されて前記データ格納部から供給された前記コンテンツキーを、前記第2のセッションキーについて復号する第2の復号処理部(1556)と、

前記データ格納部から供給された前記暗号化コンテンツデータを受けて、前記第2の復号処理部の出力に基づいて復号してコンテンツデータを抽出するための第3の復号処理部(1520)とを備える、データ再生装置。

1 3. (補正後) 前記データ再生部に固有でかつ前記固有復号鍵にて復号可能な暗号化を施すための暗号鍵である公開暗号鍵と前記データ再生部に固有な認証データとを認証鍵により復号可能な暗号化を施した上で保持し、前記データ格納部に対して出力可能な認証データ保持部(1560)をさらに備える、請求項12

***This Page Blank (uspto)***

記載のデータ再生装置。

14. (補正後) 前記データ格納部は前記データ再生装置から着脱可能である、請求項13記載のデータ再生装置。

15. (補正後) 前記コンテンツキーは、

5 前記データ再生装置に予め定められた第2の復号鍵にて復号可能な暗号化を施されて、前記記録部に格納され、

前記データ再生部は、予め定められた第2の復号鍵にて復号するための第5の復号処理部(1572)をさらに備え、

前記第5の復号処理部は、

10 前記第2の復号鍵で復号可能な暗号化を施されて、さらに、前記第2のセッションキーで暗号化された上で前記データ格納部から供給された前記コンテンツキーを、前記第2の復号処理部が前記第2のセッションキーについて復号した結果を入力として受け、前記第2の復号鍵にて復号し、前記第3の復号処理部に与える、請求項12に記載のデータ再生装置。

15 16. (補正後) 前記データ格納部は、前記データ再生装置に対して着脱可能である、請求項12に記載のデータ再生装置。

17. (補正後) 前記データ再生装置は、さらに、携帯電話網に接続するインターフェイスを備える、請求項12に記載のデータ再生装置。

18. (補正後) 前記データ再生装置は、さらに、前記インターフェイスを介して通話を行なうための通話処理部を備える、請求項17に記載のデータ再生装置。

20 19. (補正後) 前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項12に記載のデータ再生装置。

20. (補正後) 前記データ再生部は、

25 少なくとも前記鍵保持部と、前記第1の復号処理部と、前記第2の復号処理部と、前記第3の復号処理部とが、第三者には読出不可なセキュリティ領域に設けられている、請求項12に記載のデータ再生装置。

21. (補正後) 前記データ格納部(150, 160)は、

前記データ格納部に与えられるデータを格納するための記録部(1412)と、前記第1のセッションキーを発生する第2のセッションキー発生部(145

**This Page Blank (uspto)**

0) と、

前記コンテンツデータ再生部に固有でかつ前記固有復号鍵にて復号可能な暗号化を施すための公開暗号鍵により、前記第2のセッションキー発生部にて生成した前記第1のセッションキーを暗号化する第2の暗号化処理部(1452)と、

5 前記第1のセッションキーを用いて、前記データ再生部から前記第1のセッションキーにて暗号化されて伝達された前記第2のセッションキーを復号するための第4の復号処理部(1454)と、

前記第4の復号処理部にて抽出された前記第2のセッションキーにより、暗号化処理を行ない出力するための第3の暗号化処理部(1456)とを備え、

10 前記記録部に格納された前記コンテンツキーを前記第3の暗号化処理部にて暗号化して、前記データ再生部に供給する、請求項12に記載のデータ再生装置。

22. (補正後) 前記データ格納部(150, 160)は、

前記データ格納部に与えられるデータを格納するための記録部(1412)と、

15 前記認証鍵により復号可能な暗号化を施された前記公開暗号鍵と前記認証データを前記認証鍵にて復号して前記公開鍵と前記認証データを抽出するための第4の復号処理部(1460)と、

前記第4の復号処理部にて抽出された前記認証データに基づいて前記認証データを出力したデータ再生部に対して前記コンテンツキーを出力するか否か判断する認証処理の制御を行なう制御部(1420)と、

20 前記第1のセッションキーを発生する第2のセッションキー発生部(1450)と、

前記第4の復号処理部にて抽出された前記公開暗号鍵により、前記第2のセッションキー発生部にて生成した前記第1のセッションキーを暗号化する第2の暗号化処理部(1452)と、

25 前記第1のセッションキーを用いて、前記データ再生部から前記第1のセッションキーにて暗号化されて伝達された前記第2のセッションキーを復号するための第4の復号処理部(1454)と、

前記第4の復号処理部にて抽出された前記第2のセッションキーにより、暗号化処理を行ない出力するための第3の暗号化処理部(1456)とを備え、

This Page Blank (uspto)



前記記録部に格納された前記コンテンツキーを前記第 3 の暗号化処理部にて暗号化して、前記データ再生部に供給する、請求項 1 3 に記載のデータ再生装置。

2 3. (追加) 暗号化コンテンツデータを復号してコンテンツデータを再生するためのデータ再生装置に搭載するデータ再生モジュール (1 5 0 0) であって、

5 前記データ再生モジュールに固有な第 1 の復号鍵を予め保持する第 1 の鍵保持部 (1 5 4 0) と、

前記暗号化コンテンツデータを復号するための復号鍵であるコンテンツキーの取得のためのアクセスごとに前記第 2 の復号鍵により復号可能な暗号化処理を施されて前記データ再生モジュールの外部から供給される第 1 のセッションキーを、  
10 前記第 1 の復号鍵にて復号して抽出する第 1 の復号処理部 (1 5 3 0) と、

前記データ再生モジュールの外部に対して前記コンテンツキーの取得のためにアクセスするごとに更新される第 2 のセッションキーを生成するセッションキー発生部 (1 5 5 2) と、

前記第 2 のセッションキーを前記第 1 のセッションキーを用いて暗号化して前記データ再生モジュールの外部に与える暗号化処理部 (1 5 5 4) と、

前記第 2 のセッションキーで暗号化されて前記データ再生モジュールの外部から供給される前記コンテンツキーを、前記第 2 のセッションキーを用いて復号する第 2 の復号処理部 (1 5 5 6) と、

前記データ再生モジュールの外部から供給される前記暗号化コンテンツデータを受けて、前記第 2 の復号処理部の出力に基づいて復号してコンテンツデータを抽出するための第 3 の復号処理部 (1 5 2 0) とを備える、データ再生モジュール。  
20

2 4. (追加) 前記データ再生モジュールに固有でかつ前記第 1 の復号鍵にて復号可能な暗号鍵である公開暗号鍵と前記データ再生モジュールに固有な認証データとを前記データ再生モジュールの外部にて認証鍵により復号可能な暗号化を施して保持し、前記データ再生モジュールの外部に対して出力可能な認証データ保持部 (1 5 6 0) をさらに備える、請求項 2 3 に記載のデータ再生モジュール。  
25

2 5. (追加) 前記コンテンツキーは、前記第 2 のセッションキーで暗号化され前記データ再生モジュールの外部から入力され、前記第 2 の復号処理部 (1 5 5

This Page Blank (uspto)

6) は、復号結果を前記暗号化コンテンツデータを復号するためのコンテンツキーとして前記第 3 の復号処理部 (1 5 2 0) に与える、請求項 2 3 に記載のデータ再生モジュール。

2 6. (追加) 前記コンテンツキーは、前記第 1 の復号鍵にて復号可能な暗号化を施され、かつ前記第 2 のセッションキーで暗号化されて前記データ再生モジュールの外部から入力され、

前記第 1 の復号処理部は、さらに、前記第 2 の復号処理部 (1 5 5 6) の出力である前記第 1 の復号鍵にて復号可能な暗号化されたコンテンツキーを、前記第 1 の復号鍵を用いて復号し前記コンテンツキーを抽出して、前記第 3 の復号処理部 (1 5 2 0) に与える、請求項 2 3 に記載のデータ再生モジュール。

2 7. (追加) 前記コンテンツキーは、前記第 2 の復号鍵にて復号可能な暗号化を施されかつ前記第 2 のセッションキーにて暗号化されて前記データ再生モジュールの外部から入力され、

前記データ再生モジュールは、

15 前記第 2 の復号鍵を予め保持する第 2 の鍵保持部 (1 5 7 0) と、

前記第 2 の復号処理部 (1 5 5 6) から出力される前記第 2 の復号鍵にて復号可能な暗号化を施された前記コンテンツキーを前記第 2 の復号鍵を用いて復号し、前記コンテンツキーを抽出して、前記第 3 の復号処理部 (1 5 2 0) に与える第 4 の復号処理部 (1 5 7 2) とをさらに備える、請求項 2 3 に記載のデータ再生モジュール。

2 8. (追加) 前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化データであって、

前記データ再生モジュールは、

25 前記符号化データから前記符号化方式に基づいてデータを再生する再生部 (1 8 0 8) をさらに含む、請求項 2 3 に記載のデータ再生モジュール。

2 9. (追加) 前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生モジュールは、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音

This Page Blank (uspto)

楽再生部（１８０８）と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部（１５１２）とをさらに含む、請求項２３に記載のデータ再生モジュール。

５ ３０．（追加）前記データ再生モジュールは、タンパーデジスタンスモジュールである、請求項２３に記載のデータ再生モジュール。

３１．（追加）暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号してコンテンツデータを得るための復号鍵であるコンテンツキーを格納し、かつ前記暗号化コンテンツデータの取得のためにアクセスされるごとに異なる第１のセッションキーをデータ再生装置に固有な固有復号鍵により復号可能な暗号化を施して前記データ再生装置に供給するデータ記録装置（１３０，１４０，１５０，１６０）を装着して、前記データ記録装置に格納された前記暗号化コンテンツデータを、前記データ記録装置に格納されたコンテンツキーを用いて再生するためのデータ再生装置（３００，４００，５００，６００）であって、

１０

前記データ記録装置を装着し、かつ、前記データ記録装置との間でデータの授受を行なうための第１のインターフェイス（１２００）と、

１５

前記データ再生装置に固有な固有鍵を予め保持する鍵保持部（１５４０）と、  
前記コンテンツキーの取得のためのアクセスごとに更新され、かつ前記データ再生装置に固有な前記固有復号鍵により復号可能な暗号化を施されて前記データ記録装置から供給される第１のセッションキーを、前記固有復号鍵にて復号して抽出する第１の復号処理部（１５３０）と、

２０

前記データ記録装置に対する前記暗号化コンテンツキーの取得のためにアクセスするごとに更新される第２のセッションキーを生成するセッションキー発生部（１５５２）と、

前記第２のセッションキーを前記第１のセッションキーを用いて暗号化して前記データ記録装置に与えるための暗号化処理部（１５５４）と、

２５

前記第２のセッションキーで暗号化されて前記データ記録装置から供給される前記コンテンツキーを、前記第２のセッションキーを用いて復号する第２の復号処理部（１５５６）と、

前記データ記録装置から読出された前記暗号化コンテンツデータを受けて、前

This Page Blank (uspto)

記第 2 の復号処理部の出力に基づいて復号してコンテンツデータを抽出するための第 3 の復号処理部（1 5 2 0）とを備える、データ再生装置。

5 3 2. （追加）前記データ再生装置に固有でかつ、前記第 1 の復号鍵にて復号可能な暗号鍵である公開暗号鍵と前記データ再生装置に固有な認証データを前記データ記録装置にて認証鍵による復号可能な暗号化を施して保持し、前記データ記録装置に対して出力する認証データ保持部（1 5 6 0）をさらに備える、請求項 3 1 に記載のデータ再生装置。

10 3 3. （追加）前記コンテンツキーは、前記第 2 のセッションキーで暗号化されて前記データ記録装置（1 5 0）から供給され、前記第 2 の復号処理部（1 5 5 6）は、復号結果を前記暗号化コンテンツデータを復号するためのコンテンツキーとして前記第 3 の復号処理部（1 5 2 0）に与える、請求項 3 1 に記載のデータ再生装置。

15 3 4. （追加）前記コンテンツキーは、前記第 1 の復号鍵にて復号可能な暗号化を施され、かつ前記第 2 のセッションキーで暗号化されて前記データ記録装置（1 3 0, 1 4 0）から供給され、

前記第 1 の復号処理部は、さらに、前記第 2 の復号処理部（1 5 5 6）の出力である前記第 1 の復号鍵にて復号可能な暗号化されたコンテンツキーを、前記第 1 の復号鍵を用いて復号し前記コンテンツキーを抽出して、前記第 3 の復号処理部（1 5 2 0）に与える、請求項 3 1 に記載のデータ再生装置。

20 3 5. （追加）前記コンテンツキーは、前記第 2 の復号鍵にて復号可能な暗号化を施され、かつ前記第 2 のセッションキーで暗号化されて前記データ記録装置（1 6 0）から供給され、

前記データ再生装置は、

前記第 2 の復号鍵を予め保持する第 2 の鍵保持部（1 5 7 0）と、

25 前記第 2 の復号処理部（1 5 5 6）から出力される前記第 2 の復号鍵にて復号可能な暗号化を施された前記コンテンツキーを前記第 2 の復号鍵を用いて復号し、前記コンテンツキーを抽出して、前記第 3 の復号処理部（1 5 2 0）に与える第 4 の復号処理部（1 5 7 2）とをさらに備える、請求項 3 1 に記載のデータ再生装置。

**This Page Blank (uspto)**



36. (追加) 前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化データであって、

前記データ再生装置は、

5 前記符号化データから前記符号化方式に基づいてデータを再生する再生部 (1808) をさらに含む、請求項31記載のデータ再生装置。

37. (追加) 前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生装置は、前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音楽再生部 (1808) と、

10 再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部 (1512) とをさらに含む、請求項31記載のデータ再生装置。

38. (追加) 前記データ再生装置は、さらに、携帯電話網に接続する第2のインターフェイスを備える、請求項31記載のデータ再生装置。

15 39. (追加) 前記データ再生装置は、さらに、前記第2のインターフェイスを介して通話を行なうための通話処理部を備える、請求項38記載のデータ再生装置。

40. (追加) 前記データ再生装置は、

第三者には読出不可能なセキュリティ領域を備えて、

20 少なくとも前記第1の鍵保持部と、前記第1の復号処理部と、前記第2の復号処理部と、前記第3の復号処理部とが、前記セキュリティ領域に設けられている、請求項31記載のデータ再生装置。

41. (追加) 前記データ再生装置は、

第三者に読出不可能なセキュリティ領域を備えて、

25 少なくとも前記第1の鍵保持部と、前記第2の鍵保持部と、前記第1の復号処理部と、前記第2の復号処理部と、前記第3の復号処理部と、前記第2の復号処理部とが、前記セキュリティ領域に設けられている、請求項31記載のデータ再生装置。

This Page Blank (uspto)

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2001年3月8日 (08.03.2001)

PCT

(10) 国際公開番号  
WO 01/16933 A1

(51) 国際特許分類: **G10K 15/02, G06F 15/00, 17/60, H04L 9/08, 9/10, G06K 19/00, H04H 1/00, H04M 3/42, 3/493, 11/08, G10L 19/00**

(21) 国際出願番号: PCT/JP00/05832

(22) 国際出願日: 2000年8月29日 (29.08.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:  
特願平11/243583 1999年8月30日 (30.08.1999) JP  
特願平11/343707 1999年12月2日 (02.12.1999) JP

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP). 日本コロムビア株式会社 (NIPPON COLUMBIA CO., LTD.) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 Tokyo (JP). 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 畑中正行

(HATANAKA, Masayuki) [JP/JP]. 蒲田 順 (KAMADA, Jun) [JP/JP]. 畠山卓久 (HATAKEYAMA, Takahisa) [JP/JP]. 長谷部高行 (HASEBE, Takayuki) [JP/JP]. 小谷誠剛 (KOTANI, Seigou) [JP/JP]. 古田茂樹 (FURUTA, Shigeki) [JP/JP]; 〒211-8588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 穴澤健明 (ANAZAWA, Takeaki) [JP/JP]; 〒107-8011 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内 Tokyo (JP). 日置敏昭 (HIOKI, Toshiaki) [JP/JP]. 金森美和 (KANAMORI, Miwa) [JP/JP]. 堀 吉宏 (HORI, Yoshihiro) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP).

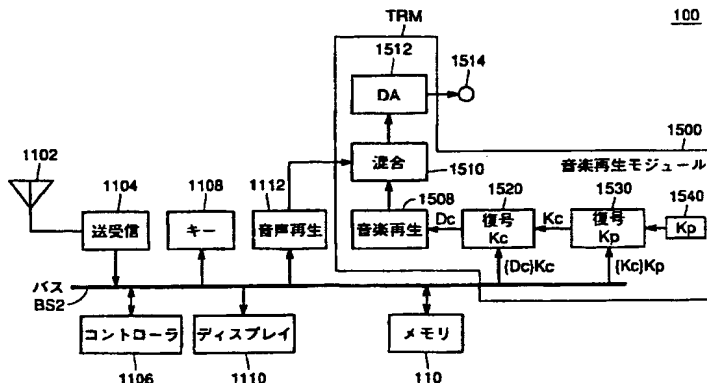
(74) 代理人: 深見久郎. 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[続葉有]

(54) Title: DEVICE FOR DATA REPRODUCTION

(54) 発明の名称: データ再生装置



110...MUSIC PLAYBACK  
1104...TRANSMISSION/RECEPTION  
1106...CONTROLLER  
1108...KEY  
1110...DISPLAY  
1112...AUDIO PLAYBACK

1500...MUSIC PLAYBACK MODULE  
1508...MUSIC PLAYBACK  
1510...MIX  
1520...DECRYPT Kc  
1530...DECRYPT Kp  
BS2...BUS

(57) Abstract: A cellular phone (100) stores distributed encrypted content data and encrypted content key in memory (110). The encrypted content key data read from the memory (110) is decrypted by decryption means (1530) using key data (kp) held by a Kp holder (1540), and then input to music playback module (1500). The encrypted content data read from the memory (110) is decrypted by decryption means (1520) using a content key (Kc) extracted by decryption means (1530), and content data (Dc) is reproduced.

[続葉有]

WO 01/16933 A1



(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

---

(57) 要約:

携帯電話機(100)は、配信された暗号化コンテンツデータおよび暗号化コンテンツキーをメモリ(110)に格納する。メモリ(110)から読み出された暗号化コンテンツキーデータは、K<sub>p</sub>保持部(1540)の保持するキーデータK<sub>p</sub>により復号処理部(1530)により復号されて、音楽再生モジュール(1500)に取り込まれる。復号処理部(1520)は、メモリ(110)から読み出した暗号化コンテンツデータを、復号処理部(1530)により抽出されたコンテンツキーK<sub>c</sub>により復号して、コンテンツデータD<sub>c</sub>を再生する。

## 明細書

## データ再生装置

## 5 技術分野

本発明は、携帯電話網等のデータ配信システムにより配送された配信データの再生装置に関し、より特定的には、配信されたデータに対する著作権保護を可能とするデータ再生装置に関するものである。

## 10 背景技術

近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

15 このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽データや画像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

20 したがって、このような情報通信網上において、音楽データや画像データ等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、か  
25 えって不利益となる。

ところで、上述したようなデジタル情報通信網を介した音楽データなどの著作権データの配信が行なわれた場合、各ユーザは、このようにして配信されたデータを何らかの記録装置に記録した上で、再生装置で再生することになる。

このような記録装置としては、たとえば、メモ리카ードのように電氣的にデー

タの書込および消去が可能な媒体が用いられることになる。

さらに、配信データを再生する装置としては、このようなデータの配信を受け  
るのに用いた携帯電話機自身を用いる場合や、あるいは、記録装置がメモリカード  
などのように配信を受ける装置から着脱可能な場合は、専用の再生装置を用い  
5 ることも可能である。

この場合、著作権者の権利保護のためには、著作権者の承諾なしに、このよう  
にして配信を受けたコンテンツデータ（音楽データ等）を自由に当該記録媒体か  
ら他の記録媒体等へ移転できないように記録媒体においてセキュリティ対策を施  
す必要がある。

10 それのみならず、このようにして正当な対価を支払った上でコンテンツデータ  
の配信を受けたユーザ以外のものが、当該記録媒体から音楽データ等の再生を行  
なう際に、再生装置側においてコンテンツデータを外部から自由に読み出すこと  
ができるとすると、著作権者の権利保護ならびに正規のユーザ側の権利保護にも  
支障を来たすことになる。

15

#### 発明の開示

本発明の目的は、配信されて記録装置に保持された音楽データ等の著作物デー  
タを再生する再生装置において、ユーザ以外の者が無断で当該著作物データに対  
してアクセスを行なうことから保護する機能を備えたデータ再生装置を提供する  
20 ことである。

係る目的を達成するために本願発明に係るデータ再生装置は、暗号化コンテン  
ツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であ  
って、データ格納部と、データ再生部とを備える。

データ格納部は、暗号化コンテンツデータおよび暗号化コンテンツデータを復  
25 号するためのコンテンツキーを暗号化した暗号化コンテンツキーを格納する。

データ再生部は、データ格納部からの出力を受けて、暗号化コンテンツデータ  
を再生する。データ再生部は、第1の鍵保持部と、第1の復号処理部と、第2の  
復号処理部とを含む。

第1の鍵保持部は、データ格納部から読み出された暗号化コンテンツキーを復

号するための第1の復号鍵を保持する。第1の復号処理部は、データ格納部からの暗号化コンテンツキーを基にして、第1の鍵保持部からの出力により復号処理を行なうことで、コンテンツキーを抽出する。第2の復号処理部は、データ格納部から読み出された暗号化コンテンツデータを受けて、第1の復号処理部の出力により復号してコンテンツデータを抽出する。

したがって、本願発明にかかるデータ再生装置によれば、正規のユーザがメモリ中に格納したコンテンツデータに対して、第三者が不当に配信データへのアクセスを行なうことが困難な構成となっているので、著作権者および正当なユーザが、無断で行なわれる不当な処理により不利益を被るのを防止することが可能となる。

#### 図面の簡単な説明

図1は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

図2は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

図3は、携帯電話機100内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

図4は、本発明の実施例2の携帯電話機200の構成を説明するための概略ブロック図である。

図5は、図4に示した携帯電話機200において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

図6は、図4に示したメモリカード120の構成を説明するための概略ブロック図である。

図7は、携帯電話機200内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

図8は、本発明の実施例3の携帯電話機300の構成を説明するための概略ブロック図である。

図9は、図8に示した携帯電話機300において使用される通信のためのキー

データ（鍵データ）等の特性をまとめて説明するための図である。

図１０は、図８に示したメモリカード１３０の構成を説明するための概略ブロック図である。

図１１は、携帯電話機３００内において、暗号化コンテンツデータから音楽を再生するための再生処理を説明するフローチャートである。

図１２は、本発明の実施例４の携帯電話機４００の構成を説明するための概略ブロック図である。

図１３は、図１２に示した携帯電話機４００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

図１４は、図１２に示したメモリカード１４０の構成を説明するための概略ブロック図である。

図１５は、メモリカード１４０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明するフローチャートである。

図１６は、本発明の実施例５の携帯電話機５００の構成を説明するための概略ブロック図である。

図１７は、図１６に示したメモリカード１５０の構成を説明するための概略ブロック図である。

図１８は、メモリカード１５０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明するフローチャートである。

図１９は、本発明の実施例６の携帯電話機６００の構成を説明するための概略ブロック図である。

図２０は、図１９に示した携帯電話機６００において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

図２１は、図１９に示したメモリカード１６０の構成を説明するための概略ブロック図である。

図２２は、メモリカード１６０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明するフローチャートである。

発明を実施するための最良の形態



以下、本発明の実施例を図面とともに説明する。

[実施例 1]

[システムの全体構成]

図 1 は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

なお、以下では携帯電話網を介して、暗号化された音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、暗号化された他の著作物情報データ、例えば画像データ等の著作物情報データを、復号して平文化して再生することが可能なものである。

なお、ここで携帯電話網としては、PHS (Personal Handy Phone) などの簡易携帯電話網も含むものとする。

図 1 を参照して、著作権の存在する音楽データを管理する配信サーバ 10 は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリア 20 である携帯電話会社に、このような暗号化データを与える。

配信キャリア 20 は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）を配信サーバ 10 に中継する。配信サーバ 10 は、配信リクエストがあると、要求された暗号化音楽情報を携帯電話会社 20 の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

さらに、たとえばユーザ 1 は、携帯電話機 100 に接続したヘッドホン 140 等を介してこのような再生された音楽データを聴取することが可能である。

以下では、このような配信サーバ 10 と配信キャリア（携帯電話会社）20 とを併せて、音楽サーバ 30 と総称することにする。

また、このような音楽サーバ 30 から、各携帯電話端末等に音楽情報を伝送する処理を「配信」と称することとする。

しかも、配信キャリア 20 において、たとえば 1 曲分の音楽データを配信するたびにその度数を計数しておくことで、ユーザが著作物データを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア 20 が携帯電話機の通話料

金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

しかも、このような著作物データの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

#### [配信サーバ10の構成]

図1において配信サーバ10は、音楽データ（コンテンツデータ）を所定的方式に従って暗号化したコンテンツデータやコンテンツキー等の配信情報を保持するための配信情報データベース304と、各ユーザごとに音楽情報へのアクセス回数等に従った課金情報を保持するための課金データベース302と、暗号化コンテンツデータを復号するためのコンテンツキーKcを公開暗号化鍵Kpにより暗号化するためのコンテンツキー暗号化処理部316と、配信情報データベース304および課金データベース302とデータバスBS1を介してデータ授受を行ない、配信サーバ10の動作を制御するためのコントローラ312と、通信網を介して、配信サーバ10と配信キャリア20との間でデータ授受を行なうための通信装置350とを備える。

すなわち、配信情報データベース304からは、コンテンツデータDcが復号鍵であるコンテンツキーKcにより復号可能な状態に暗号化された暗号化コンテンツデータ[Dc]Kcと、コンテンツキーKcとが出力される。コントローラ312は、コンテンツキー暗号化処理部316を制御して、このコンテンツキーKcを公開暗号化鍵Kpにより暗号化した[Kc]Kpを通信装置350を介して、配信キャリア20に与える。

ここで、[Y]Xという表記は、データYを、キー（鍵）Xにより復号可能な暗号に変換したデータであることを示している。なお、暗号化処理、復号処理で用いられる鍵を、「キー」とも称することとする。

#### [端末（携帯電話機）の構成]

図2は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

携帯電話機100は、携帯電話網により無線伝送される信号を受信するための

アンテナ 1102 と、アンテナ 1102 からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ 1102 に与えるための送受信部 1104 と、携帯電話機 100 の各部のデータ授受を行なうためのデータバス BS2 と、データバス BS2 を介して携帯電話機 100 の動作を制御するためのコントローラ 1106 と、外部からの指示を携帯電話機 100 に与えるためのタッチキーやダイヤルキーなどを含むキーボード 1108 と、コントローラ 1106 等から出力される情報をユーザに視覚情報として与えるためのディスプレイ 1110 と、通常の通話動作において、データバス BS2 を介して与えられる受信データに基づいて音声を再生するための音声再生部 1112 とを備える。

携帯電話機 100 は、さらに、サーバ 30 からの暗号化コンテンツデータ [Dc] Kc および暗号化コンテンツキー [Kc] Kp を格納するためのメモリ 110 と、音楽再生モジュール 1500 とを備える。この音楽再生モジュール 1500 は、公開暗号化鍵 Kp に対応し、キー Kp で暗号化されたデータを復号可能な秘密復号鍵 Kp を保持する Kp 保持部 1540 と、音楽サーバ 30 から伝送され公開暗号化鍵 Kp により暗号化コンテンツキー [Kc] Kp をメモリ 110 から受けて復号するための復号処理部 1530 と、音楽サーバ 30 から配信されメモリ 110 中に格納された暗号化コンテンツデータ [Dc] Kc を、復号処理部 1530 で復号抽出されたコンテンツキー Kc に基づいて復号するための復号処理部 1520 と、復号処理部 1520 からの復号されたコンテンツデータを受けて、コンテンツデータを符号化した符号化方式、例えば、MP3 (MPEG1 Audio Layer III)、AC3 等のデジタル圧縮符号化方式の再生手順に従って音楽データを再生するための音楽再生部 1508 と、音楽再生部 1508 の出力と音声再生部 1112 の出力とを受けて、動作モードに応じて選択的に出力、または、両者を混合して出力するための混合部 1510 と、混合部 1510 の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部 1512 とを含む。

携帯電話機 100 は、さらに、デジタルアナログ変換部 1512 の出力を受けて、ヘッドホン 140 と接続するための接続端子 1514 とを含む。

なお、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

また、図2に示した構成において、音楽再生部1508、Kp保持部1540、  
5 復号処理部1530および復号処理部1520を、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組み込む構成とすることが可能である。このようなモジュールは、一般にはタンパーレジスタンスモジュール (Tamper Resistance Module) と呼ばれる。

10 このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機100の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

さらに、図2において実線で囲んだ領域に相当する音楽再生モジュール1500を、TRMとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが可能である。

#### [再生処理]

図3は、携帯電話機100内において、メモリ110に保持された暗号化コンテンツデータから、コンテンツデータを復号して、音楽として外部に出力するための再生処理を説明するフローチャートである。

図3を参照して、携帯電話のキーボード1108等からのユーザの指示により、再生リクエストがコントローラ1106に与えられる (ステップS100)。

この再生リクエストに応じて、コントローラ1106は、メモリ110を制御して暗号化コンテンツキー [Kc] Kpを読み出す (ステップS102)。

25 つづいて、復号処理部1530は、メモリ110から読み出された暗号化コンテンツキー [Kc] Kpに対する復号処理を行なう (ステップS104)。

復号処理部1530においてコンテンツキーKcを復号抽出可能な場合は (ステップS106)、処理は次のステップに移行し、一方、復号不能と判断された場合は、処理は終了する (ステップS110)。

復号処理部 1 5 3 0 においてコンテンツキー K c を復号抽出可能な場合は、コントローラ 1 1 0 8 は、メモリ 1 1 0 を制御して、暗号化コンテンツデータ [D c] K c を読み出して、復号処理部 1 5 2 0 に与え、復号処理部 1 5 2 0 は、復号鍵 K c により復号処理して、平文化したコンテンツデータ D c を生成して音楽再生部 1 5 0 8 に与える。音楽再生部 1 5 0 8 においてコンテンツデータ D c より再生された音楽信号は、混合部 1 5 1 0 を経由して、デジタルアナログ変換器 1 5 1 2 によりアナログ信号に変換されて接続端子 1 5 1 4 から外部に出力される。

以上のような構成とすることで、再生装置である携帯電話機 1 0 0 内のメモリ 1 1 0 には、暗号化コンテンツデータと暗号化コンテンツキーが保持されているのみであるため、外部からこのメモリ 1 1 0 内の記憶内容を仮に読み出したとしても、音楽を再生することはできない。

しかも、メモリ 1 1 0 から復号処理部 1 5 2 0 および 1 5 3 0 に与えられるデータも、このような暗号化されたデータであるため、データバス B S 2 上の信号を外部から仮に検出したとしても、音楽を再生することはできない。

さらに、平文化された音楽データが伝達される部分は、上述のとおり、タンパレージスタンスモジュールで構成されているので、この部分から音楽データを外部に読み出すこともできない構成となっている。

したがって、図 2 に示した携帯電話機 1 0 0 の構成により、不正な手続きでコンテンツデータを複製して、再生あるいは配布を行なうことから保護することが可能となる。

#### [実施例 2]

図 4 は、本発明の実施例 2 の携帯電話機 2 0 0 の構成を説明するための概略ブロック図であり、実施例 1 の図 2 と対比される図である。

図 2 に示した携帯電話機 1 0 0 の構成と、携帯電話機 2 0 0 の構成が異なる点は、以下のとおりである。

まず、図 4 においては、携帯電話機 2 0 0 には、携帯電話機 2 0 0 により受信された暗号化コンテンツデータを受取って格納し、暗号化コンテンツデータおよび暗号化コンテンツキーをさらに所定の暗号化処理をした上で、携帯電話機 2 0

0中の音楽再生モジュール1500に与えるための着脱可能なメモリカード120が装着される構成となっている。これに応じて、携帯電話機200は、メモリカード120とデータバスBS2との間のデータの授受を制御するためのメモリインタフェース1200をさらに備えている。

5       さらに、携帯電話機200の構成では、音楽再生モジュール1500の構成も、携帯電話機100の構成と異なる。

すなわち、携帯電話機200の音楽再生モジュール1500は、メモリカード120と携帯電話機の他の部分とのデータ授受にあたり、データバスBS2上においてやり取りされるデータを暗号化するための後に説明するセッションキーKsを乱数等により発生するセッションキー発生部1502と、セッションキー発生部1502により生成されたセッションキーKsを暗号化して、データバスBS2に与えるための暗号化処理部1504と、データバスBS2によりメモリカード120から伝送され、公開暗号化鍵KppおよびセッションキーKsにより暗号化コンテンツキーKcをセッションキーKsについて復号して出力する復号処理部1506と、公開暗号化鍵Kppに対応し、キーKppで暗号化されたデータを復号可能な秘密復号鍵Kpを保持するKp保持部1540と、復号処理部1506の出力を受けて、メモリカード120から伝送され公開暗号化鍵Kppにより暗号化コンテンツキー[Kc]Kpを復号するための復号処理部1530と、サーバ30から配信されメモリカード120中に格納された暗号化コンテンツデータ[Dc]Kcを、復号処理部1530で復号抽出されたコンテンツキーKcに基づいて復号するための復号処理部1520と、復号処理部1520からの復号されたコンテンツデータDcを受けて、音楽サーバ30から配信された音楽データを再生するための音楽再生部1508と、音楽再生部1508の出力と音声再生部1112の出力とを受けて、動作モードに応じて選択的に出力、または、両者を混合して出力するための混合部1510と、混合部1510の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部1512とを含む。

10  
15  
20  
25

携帯電話機200のその他の部分は、実施例1の携帯電話機100の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図4においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

また、図4に示した構成において、音楽再生部1508、K<sub>p</sub>保持部1540、  
5 復号処理部1530、復号処理部1520、復号処理部1506、暗号化処理部  
1504およびK<sub>s</sub>発生部1502を、TRMに組み込む構成とすることが可能  
である。

このような構成とすることで、すくなくとも、復号鍵および平文化されたデー  
タを外部から参照できないため、携帯電話機200の暗号化方式および秘密復号  
10 鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

さらに、図4において実線で囲んだ領域に相当する音楽再生モジュール150  
0を、TRMとすることも可能である。このような構成とすれば、音楽データ等  
の著作権の存在するコンテンツデータの最終的なデジタルデータについても、保護  
することが可能である。

#### 15 [暗号／復号鍵の構成]

図5は、図4に示した携帯電話機200において使用される通信のためのキー  
データ（鍵データ）等の特性をまとめて説明するための図である。

まず、図4に示した構成において、メモ리카ード120内のデータ処理を管理  
するための鍵としては、メモ리카ードに固有な公開暗号化鍵K<sub>Pm</sub>と、公開暗号  
20 化鍵K<sub>Pm</sub>により暗号化されたデータを復号するためのキーK<sub>Pm</sub>とは非対称な  
秘密復号鍵K<sub>m</sub>とがある。

ここで、キーK<sub>Pm</sub>とキーK<sub>m</sub>とが非対称とは、複数の公開暗号化鍵K<sub>Pm</sub>に  
より暗号化されたデータが、キーK<sub>Pm</sub>とは異なりK<sub>Pm</sub>からは容易に類推でき  
ない復号鍵K<sub>m</sub>により復号できることを意味する。

したがって、メモ리카ード120と携帯電話機200とのセッションキーの授  
25 受にあたっては、後に説明するようにこれら暗号化鍵K<sub>m</sub>、復号鍵K<sub>Pm</sub>が用い  
られることになる。

さらに、メモ리카ード外でのデータの授受における秘密保持のための暗号化鍵  
としては、携帯電話機という再生装置に固有な公開暗号化鍵をK<sub>Pp</sub>と、音楽再

生モジュール管理の鍵として、このキー $K_P p$ で暗号化されたデータを復号化でき、キー $K_P p$ とは非対称な秘密復号鍵 $K_p$ と、各通信ごとに $K_s$ 発生器1502において生成される共通鍵 $K_s$ とが用いられる。

5      ここで、共通鍵 $K_s$ は、たとえば、携帯電話機200とメモ리카ード120との間のコンテンツデータの授受のためのアクセスが行なわれるごとに $K_s$ 発生器1502において発生する。

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵 $K_s$ を「セッションキー」とも呼ぶことにする。

10      したがって、セッションキー $K_s$ は各通信セッションに固有の値を有することになり、音楽再生モジュール1500において管理される。

さらに、メモ리카ード120に記録される著作物データについては、まず、コンテンツデータ（音楽データ）自体を暗号化するための共通鍵であるコンテンツキー $K_c$ があり、このコンテンツキー $K_c$ により暗号化コンテンツデータが復号（平文化）されるものとする。

15      著作権の存在するコンテンツデータ $D_c$ は、上述のとおり、たとえば音楽データであり、このコンテンツデータをコンテンツキー $K_c$ で復号化可能なデータを、暗号化コンテンツデータ $[D_c] K_c$ と呼ぶ。

また、配信サーバ10から携帯電話機200に向けて、コンテンツキー $K_c$ が配信される場合には、このコンテンツキー $K_c$ は、すくなくとも公開暗号化鍵 $K_P p$ により暗号化されており、メモ리카ード120中には、この暗号化コンテンツキー $[K_c] K_p$ として格納されているものとする。

[メモ리카ードの構成]

図6は、図4に示したメモ리카ード120の構成を説明するための概略ブロック図である。

25      メモ리카ード120は、メモリアインタフェース1200との間で信号を端子1202を介して授受するデータバス $B_S 3$ と、公開暗号化鍵 $K_P m$ の値を保持し、データバス $B_S 3$ に公開暗号化鍵 $K_P m$ を出力するための $K_P m$ 保持部1401と、カード120に対応する秘密復号鍵 $K_m$ を保持するための $K_m$ 保持部1402と、データバス $B_S 3$ にメモリアインタフェース1200から与えられるデータ



から、秘密復号鍵 $K_m$ により復号処理をすることにより、セッションキー $K_s$ を抽出する復号処理部1404と、データベースBS3から、公開暗号化鍵 $K_p$ で暗号化されているコンテンツキー $K_c$ およびコンテンツキー $K_c$ により暗号化されている暗号化コンテンツデータ $[D_c]$   $K_c$ を受けて格納するためのメモリ1412と、復号処理部1404により抽出されたセッションキー $K_s$ に基づいて、メモリ1412からの出力を暗号化してデータベースBS3に与えるための暗号化処理部1406と、メモリカード120の動作を制御するためのコントローラ1420とを備える。

なお、図6のメモリカード120内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれる構成とすることも可能である。

#### [再生処理]

図7は、携帯電話機200内において、メモリカード120に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図7を参照して、携帯電話機のキーボード1108等からのユーザの指示により、再生リクエストがメモリカード120に対して出力される（ステップS200）。

メモリカード120においては、この再生リクエストに応じて、コントローラ1420は、 $K_{Pm}$ 保持部1401から、データベースBS3、端子1202およびメモリインタフェース1200を介して、公開暗号化鍵 $K_{Pm}$ を携帯電話機200に対して送信する（ステップS202）。

携帯電話機200では、カード120からのキー $K_{Pm}$ を受信すると（ステップS204）、 $K_s$ 発生部1502においてセッションキー $K_s$ を生成し（ステップS206）、暗号化処理部1504が、キー $K_{Pm}$ により、セッションキー $K_s$ を暗号化して暗号化セッションキー $[K_s]$   $K_{Pm}$ を生成し、データベースBS2を介して、カード120に対して送信する（ステップS208）。

メモリカード120は、携帯電話機200により生成された暗号化セッション

キー [K s] K P mを受け取り、復号処理部 1 4 0 4 において秘密復号鍵 K m により復号し、セッションキー K s を抽出する（ステップ S 2 1 0）。

続いて、メモリカード 1 2 0 は、メモリ 1 4 1 2 から、コンテンツキー [K c] K p を読出す（ステップ S 2 1 2）。

- 5        続いて、メモリカード 1 2 0 は、暗号化処理部 1 4 0 6 において抽出したセッションキー K s により、暗号化コンテンツキー [K c] K p を暗号化し、暗号化された暗号化コンテンツキー [ [K c] K p ] K s をデータバス B S 2 に与える（ステップ S 2 1 4）。

- 10       携帯電話機 2 0 0 の復号処理部 1 5 0 6 は、メモリカード 1 2 0 から送信された暗号化された暗号化コンテンツキー [ [K c] K p ] K s をセッションキー K s により復号処理を行なうことにより、暗号化コンテンツキー [K c] K p を取得する（ステップ S 2 1 6）。

- 15       さらに、携帯電話機 2 0 0 の復号処理部 1 5 3 0 は、K p 保持部 1 5 4 0 からのキー K p に基づいて、データ [K c] K p の復号処理を行なう（ステップ S 2 1 8）。

復号処理部 1 5 3 0 が復号処理により、コンテンツキー K c を抽出できた場合は（ステップ S 2 2 0）、処理は次のステップ S 2 2 2 に進み、抽出できない場合は（ステップ S 2 2 0）、処理は終了する（ステップ S 2 2 6）。

- 20       復号処理部 1 5 3 0 が復号処理により、コンテンツキー K c を抽出できた場合は、メモリカード 1 2 0 は、暗号化コンテンツデータ [D c] K c をメモリ 1 4 1 2 から読出し、データバス B S 2 に与える（ステップ S 2 2 2）。

- 25       携帯電話機 2 0 0 の復号処理部 1 5 2 0 は、暗号化コンテンツデータ [D c] K c を、抽出されたコンテンツキー K c により復号処理して平文のコンテンツデータ D c を生成し、音楽再生部 1 5 0 8 は、コンテンツデータ D c を再生して混合部 1 5 1 0 に与える。デジタルアナログ変換部 1 5 1 2 は、混合部 1 5 1 0 からのデータを受け取ってアナログ信号に変換し、外部に再生された音楽を出力し、処理が終了する（ステップ S 2 2 6）。

このような構成とすることで、携帯電話機 2 0 0 において生成されたセッションキーに基づいてコンテンツキーを暗号化した上で、メモリカード 1 2 0 から携

携帯電話機 200 に送信して再生動作を行なうことが可能となる。

以上のような構成により、実施例 1 の携帯電話機 100 の奏する効果に加えて、実施例 2 の携帯電話機 200 においては、携帯電話機 200 に対して、着脱可能なメモ리카ード内に配信データが格納される構成となっているので、配信を受けたり、再生する際にのみメモ리카ードを装着すれば足りるため、重量等の観点から携帯機としての利便性が損なわれることがない。

しかも、携帯電話機とメモ리카ードとの間のデータの授受は、セッションキーにより暗号化された上で行なわれるので、データに対するセキュリティが向上し、著作権者およびユーザの双方の権利を保護することが可能となる。

さらに、配信を受けた後は、メモ리카ードをほかの再生装置に装着することで、再生を行なうことも可能となり、ユーザの音楽データ利用の自由度が向上する。

#### [実施例 3]

図 8 は、本発明の実施例 3 の携帯電話機 300 の構成を説明するための概略ブロック図であり、実施例 2 の図 4 と対比される図である。

図 8 に示した実施例 3 の携帯電話機 300 の構成と、実施例 2 の携帯電話機 200 の構成が異なる点は、以下のとおりである。

まず、図 8 においては、携帯電話機 300 には、携帯電話機 300 により受信された暗号化された音楽データを受取って格納し、暗号化コンテンツデータおよび暗号化コンテンツキーをさらに所定の暗号化処理をした上で、携帯電話機 300 中の音楽再生モジュール 1500 に与えるための着脱可能なメモ리카ード 130 が装着される構成となっている。

メモ리카ード 130 は、後に説明するように、メモ리카ード 130 自身でセッションキー  $K_s 2$  を生成する点で、メモ리카ード 120 と異なる。

さらに、携帯電話機 300 の構成では、音楽再生モジュール 1500 の構成も、携帯電話機 200 の構成と異なる。

すなわち、携帯電話機 300 の音楽再生モジュール 1500 は、メモ리카ード 130 と携帯電話機の他の部分とのデータ授受にあたり、データバス  $BS 2$  上においてやり取りされるデータを暗号化するためのセッションキー  $K_s 1$  を乱数等により発生するセッションキー発生部 1552 と、セッションキー発生部 155

2により生成されたセッションキー $K_s1$ をメモリカード130からのセッションキー $K_s2$ で暗号化して、データバスBS2に与えるための暗号化処理部1554と、データバスBS2によりメモリカード130から伝送され、公開暗号化鍵 $K_{pp}$ およびセッションキー $K_s1$ により暗号化コンテンツキー $K_c$ をセッションキー $K_s1$ について復号して出力する復号処理部1556と、コントローラ1106により制御されて、データバスBS2により伝達された暗号化されたメモリカード130のセッションキー $[K_s2]$  $K_p$ または復号処理部1556から出力された暗号化コンテンツキー $[K_c]$  $K_p$ のいずれかを、公開暗号化鍵 $K_{pp}$ により暗号化されたデータを復号するための復号処理部1530に与える切換え回路1550とを含む。

暗号化処理部1554は、復号処理部1530において秘密復号鍵 $K_p$ により復号されて抽出されたメモリカード130のセッションキー $K_s2$ を受けて、セッションキー発生部1552により生成されたセッションキー $K_s1$ をセッションキー $K_s2$ で暗号化処理する。

携帯電話機300のその他の部分は、実施例2の携帯電話機200の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図8においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

また、図8に示した構成において、音楽再生部1508、 $K_p$ 保持部1540、復号処理部1530、復号処理部1520、復号処理部1556、暗号化処理部1554、セッションキー発生部1552および切換え回路1550を、TRMに組み込む構成とすることが可能である。

このような構成とすることで、すくなくとも、復号鍵および平文化されたデータを外部から参照できないため、携帯電話機300の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

さらに、図8において実線で囲んだ領域に相当する音楽再生モジュール1500を、TRMとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するコンテンツデータの最終的なデジタルデータについても、保護

することが可能である。

[暗号／復号鍵の構成]

図9は、図8に示した携帯電話機300において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

5       まず、図8に示した構成において、メモ리카ード130内のデータ処理を管理するための鍵としては、メモ리카ードに固有な公開暗号化鍵 $K_{Pm}$ と、公開暗号化鍵 $K_{Pm}$ により暗号化されたデータを復号するためのキー $K_{Pm}$ とは非対称な秘密復号鍵 $K_m$ と、メモ리카ード130が生成し各セッションに固有なセッションキー $K_{s2}$ とがある。

10       したがって、メモ리카ード130と携帯電話機300とのセッションキーの授受にあたっては、後に説明するようにこれら暗号鍵 $K_m$ 、復号鍵 $K_{Pm}$ 、セッションキー $K_{s2}$ が用いられることになる。

さらに、メモ리카ード外でのデータの授受における秘密保持のための暗号鍵としては、携帯電話機という再生装置に固有な公開暗号化鍵であって、コンテンツデータの配信時にコンテンツデータとともに配信され、後に説明するようにメモ  
15       리카ード130内に記憶される公開暗号鍵 $K_{Pp}$ と、音楽再生モジュールの管理の鍵として、このキー $K_{Pp}$ で暗号化されたデータを復号化でき、キー $K_{Pp}$ とは非対称な秘密復号鍵 $K_p$ と、各アクセスごとにセッションキー発生器1552において生成される共通鍵であるセッションキー $K_{s1}$ とが用いられる。

20       セッションキー $K_{s1}$ も各通信セッションに固有の値を有することになり、音楽再生モジュール1500において管理される。

さらに、メモ리카ード130に記録される著作物データについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるコンテンツ  
25       キー $K_c$ があり、このコンテンツキー $K_c$ により暗号化コンテンツデータが復号（平文化）されるものとする。

また、配信サーバ10から携帯電話機300に向けて、コンテンツキー $K_c$ が配信される場合には、このコンテンツキー $K_c$ は、すくなくとも公開暗号化鍵 $K_{Pp}$ により暗号化されており、メモ리카ード130中には、この暗号化コンテンツキー $[K_c] K_p$ として格納されているものとする。

さらに、著作権の存在するコンテンツデータ  $D_c$  は、このコンテンツデータをコンテンツキー  $K_c$  で復号化可能な暗号化コンテンツデータ  $[D_c] K_c$  としてメモ리카ード 130 に格納されているものとする。

〔メモ리카ードの構成〕

5 図10は、図8に示したメモ리카ード130の構成を説明するための概略ブロック図である。

メモ리카ード130は、メモリアインタフェース1200との間で信号を端子1202を介して授受するデータバスBS3と、セッション毎にセッションキー  $K_s$  2を生成するためのセッションキー発生部1450と、セッションキー  $K_s$  2を公開暗号化鍵  $K_P$  pで暗号化してデータバスBS3に与えるための暗号化処理部1452と、データバスBS3にメモリアインタフェース1200から与えられるデータ  $[K_s 1] K_s$  2から、セッションキー  $K_s$  2により復号処理をすることにより、携帯電話機300からのセッションキー  $K_s$  1を抽出する復号処理部1454と、データバスBS3から、公開暗号化鍵  $K_P$  pと、公開暗号化鍵  $K_P$  pで暗号化されているコンテンツキー  $[K_c] K_p$  とコンテンツキー  $K_c$  により暗号化されている暗号化コンテンツデータ  $[D_c] K_c$  との3つを受けて格納するためのメモリ1412と、復号処理部1454により抽出されたセッションキー  $K_s$  1に基づいて、メモリ1412からの出力を暗号化してデータバスBS3に与えるための暗号化処理部1456と、メモ리카ード130の動作を制御するためのコントローラ1420とを備える。

なお、図10のメモ리카ード130内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組み込まれる構成とすることも可能である。

25 〔再生処理〕

図11は、携帯電話機300内において、メモ리카ード130に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図11を参照して、携帯電話機のキーボード1108等からのユーザの指示に

より、再生リクエストがメモリカード130に対して出力される（ステップS300）。

メモリカード130においては、この再生リクエストに応じて、コントローラ1420は、セッションキー発生部1450を制御してセッションキーKs2を発生させる（ステップS302）。コントローラ1420の制御により、このセッションキーKs2を暗号化処理部1452は公開暗号化鍵Kpにより暗号化して暗号化セッションキー[Ks2]Kpを生成し、この暗号化セッションキー[Ks2]Kpを、データバスBS3、端子1202およびメモリインタフェース1200を介して、携帯電話機300に対して送信する（ステップS304）。

携帯電話機300では、カード130からの暗号化セッションキー[Ks2]Kpを受信すると、切換え回路1550を介して復号処理部1530が暗号化セッションキー[Ks2]Kpを受けて復号しセッションキーKs2を獲得する（ステップS306）。

携帯電話機300においては、セッションキー発生部1552においてセッションキーKs1を生成し（ステップS308）、暗号化処理部1554が、ステップS306において抽出されたセッションキーKs2により、セッションキーKs1を暗号化して暗号化セッションキー[Ks1]Ks2を生成し、データバスBS2を介して、カード130に対して送信する（ステップS310）。

メモリカード130は、携帯電話機300により生成され、かつ暗号化されたセッションキー[Ks1]Ks2を受け取り、復号処理部1454においてセッションキーKs2により復号し、セッションキーKs1を抽出する（ステップS312）。

続いて、メモリカード130は、メモリ1412から、暗号化コンテンツキー[Kc]Kpを読み出し（ステップS314）、暗号化処理部1456において、抽出したセッションキーKs1により、暗号化コンテンツキー[Kc]Kpを暗号化し、暗号化された暗号化コンテンツキー[[Kc]Kp]Ks1をデータバスBS3等を介してデータバスBS2に与える（ステップS316）。

携帯電話機300の復号処理部1556は、メモリカード130から送信された暗号化された暗号化コンテンツキー[[Kc]Kp]Ks1に対してセッショ

ンキーK<sub>s1</sub>により復号処理を行なうことにより、暗号化コンテンツキー[K<sub>c</sub>]K<sub>p</sub>を取得する(ステップS318)。

- 5 さらに、携帯電話機300の復号処理部1530は、切換え回路1550を介して暗号化コンテンツキー[K<sub>c</sub>]K<sub>p</sub>を受け、K<sub>p</sub>保持部1540からのキーK<sub>p</sub>に基づいて、暗号化コンテンツキー[K<sub>c</sub>]K<sub>p</sub>の復号処理を行なう(ステップS320)。

復号処理部1530が復号処理により、コンテンツキーK<sub>c</sub>を抽出できた場合は(ステップS322)、処理は次のステップS324に進み、抽出できない場合は(ステップS322)、処理は終了する(ステップS330)。

- 10 復号処理部1530が復号処理により、コンテンツキーK<sub>c</sub>を抽出できた場合は、メモ리카ード130は、暗号化コンテンツデータ[D<sub>c</sub>]K<sub>c</sub>をメモリ1412から読出し、データバスBS3等を介してデータバスBS2に与える(ステップS324)。

- 15 携帯電話機300の復号処理部1520は、暗号化コンテンツデータ[D<sub>c</sub>]K<sub>c</sub>を、抽出されたコンテンツキーK<sub>c</sub>により復号処理して平文のコンテンツデータD<sub>c</sub>を生成し、音楽再生部1508は、コンテンツデータD<sub>c</sub>を再生して混合部1510に与える。デジタルアナログ変換部1512は、混合部1510からのデータを受け取ってアナログ信号に変換し、外部に再生された音楽を出力し(ステップS328)、処理が終了する(ステップS330)。

- 20 このような構成とすることで、携帯電話機300において生成されたセッションキーK<sub>s1</sub>に基づいて暗号化コンテンツキー[K<sub>c</sub>]K<sub>p</sub>を暗号化した上で、メモ리카ード130から携帯電話機300に送信して再生動作を行なうことが可能となる。しかも、メモ리카ード130においてセッション毎に生成されたセッションキーK<sub>s2</sub>により暗号化した上で、メモ리카ード130と携帯電話機300との間でセッションキーK<sub>s1</sub>の授受が行なわれるので、実施例2よりも一層、  
25 セキュリティが向上し、著作権者およびユーザの双方の権利を保護することが可能となる。

また、以上のような構成により、実施例3の携帯電話機300においても、携帯電話機300に対して、着脱可能なメモ리카ード内に配信データが格納される



構成となっているので、配信を受けたり、再生する際にのみメモリカードを装着すれば足りるため、重量等の観点から携帯機としての利便性が損なわれることがない。

- 5 さらに、配信を受けた後は、メモリカードをほかの再生装置に装着することで、再生を行なうことも可能となり、ユーザの音楽データ利用の自由度が向上する。

[実施例 4]

図 1 2 は、本発明の実施例 4 の携帯電話機 4 0 0 の構成を説明するための概略ブロック図であり、実施例 3 の図 8 と対比される図である。

- 10 図 1 2 に示した実施例 4 の携帯電話機 4 0 0 の構成と、実施例 3 の携帯電話機 3 0 0 の構成が異なる点は、以下のとおりである。

- すなわち、図 1 2 においては、携帯電話機 4 0 0 には、携帯電話機 4 0 0 により受信された暗号化コンテンツデータおよび暗号化コンテンツキーを受取って格納し、さらに所定の暗号化処理をした上で、携帯電話機 4 0 0 中の音楽再生モジュール 1 5 0 0 に与えるための着脱可能なメモリカード 1 4 0 が装着される構成  
15 となっている。メモリカード 1 4 0 は、後に説明するように、携帯電話機 4 0 0 に対する認証機能を有する点で実施例 3 のメモリカード 1 3 0 と異なる。

さらに、携帯電話機 4 0 0 の構成では、音楽再生モジュール 1 5 0 0 の構成も、携帯電話機 3 0 0 の構成と異なる。

- すなわち、携帯電話機 4 0 0 の音楽再生モジュール 1 5 0 0 は、メモリカード 1 4 0 と携帯電話の他の部分とのデータ授受にあたり、携帯電話機 4 0 0 に対する認証機能を実現するために、再生装置である携帯電話機 4 0 0 のクラス（種類等）に固有な公開暗号鍵  $K P p$  と認証データ  $C r t f$  とを、システムに共通な公開復号鍵（公開認証鍵）  $K P m a$  により暗号化して保持する [ $K P p$ 、 $C r t f$ ]  
20  $K P m a$  保持部 1 5 6 0 をさらに備える構成となっている点である。

- 25 携帯電話機 4 0 0 のその他の部分は、実施例 3 の携帯電話機 3 0 0 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図 1 2 においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

また、図 1 2 に示した構成において、音楽再生部 1 5 0 8、K p 保持部 1 5 4 0、復号処理部 1 5 3 0、復号処理部 1 5 2 0、復号処理部 1 5 5 6、暗号化処理部 1 5 5 4、セッションキー発生部 1 5 5 2、切換え回路 1 5 5 0 および [K P p、C r t f] K P m a 保持部 1 5 6 0 を、T R M に組み込む構成とすることが可能である。

このような構成とすることで、すくなくとも、認証データ、復号鍵および平文化されたデータを外部から変更あるいは参照できないため、携帯電話機 4 0 0 の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキュリティが向上する。

さらに、図 1 2 において実線で囲んだ領域に相当する音楽再生モジュール 1 5 0 0 を、T R M とすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが可能である。

#### [暗号／復号鍵の構成]

図 1 3 は、図 1 2 に示した携帯電話機 4 0 0 において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

まず、図 1 2 に示した構成において、メモ리카ード 1 4 0 内のデータ処理を管理するための鍵としては、システムに共通な公開復号鍵であり、認証鍵の機能を有する K P m a と、メモ리카ード 1 4 0 が生成し各セッションに固有な共通鍵であるセッションキー K s 2 とがある。

さらに、メモ리카ード外でのデータの授受における秘密保持のための暗号鍵としては、音楽再生モジュールの管理の鍵として、携帯電話機という再生装置のクラスに固有な公開暗号化鍵であって、上述のとおり、鍵 K P m a により暗号化された形で携帯電話機 4 0 0 中の [K P p、C r t f] K P m a 保持部 1 5 6 0 に格納されている公開暗号鍵 K P p と、このキー K P p で暗号化されたデータを復号化でき、キー K P p とは非対称な秘密復号鍵 K p と、各アクセスごとにセッションキー発生器 1 5 5 2 において生成される共通鍵であるセッションキー K s 1 とが用いられる。

セッションキー K s 1 も各通信セッションに固有の値を有することになり、音

楽再生モジュール1500において管理される。

なお、「再生装置のクラス」とは、再生装置ごと、あるいは、再生装置の種類（製造メーカ、製造ロット）ごとに、この再生装置を区別するための区分であるものとする。

- 5       さらに、メモリカード140に記録される著作物データについては、まず、コンテンツデータ（音楽データ）自体を暗号化するための共通鍵であるコンテンツキー $K_c$ があり、このコンテンツキー $K_c$ により暗号化コンテンツデータが復号（平文化）されるものとする。

- 10       また、配信サーバ10から携帯電話機400に向けて、コンテンツキー $K_c$ が配信される場合には、このコンテンツキー $K_c$ は、すくなくとも公開暗号化鍵 $K_{Pp}$ により暗号化されており、メモリカード140中には、この暗号化コンテンツキー $[K_c] K_p$ として格納されているものとする。

- 15       さらに、著作権の存在するコンテンツデータ $D_c$ は、このコンテンツデータをコンテンツキー $K_c$ で復号化可能な暗号化コンテンツデータ $[D_c] K_c$ としてメモリカード140に格納されているものとする。

[メモリカードの構成]

図14は、図12に示したメモリカード140の構成を説明するための概略ブロック図である。

- 20       メモリカード140の構成が、実施例3のメモリカード130の構成と異なる点は、まず、コントローラ1420に制御されて、データバスBS3上のデータに対して公開復号鍵 $K_{Pma}$ による復号処理を行い、携帯電話機140からの公開暗号鍵 $K_{Pp}$ および認証データ $Crtf$ の取得を行うための復号処理部1460を備える構成となっている点である。したがって、暗号化処理部1452は、復号処理部1460からの公開暗号化鍵 $K_{Pp}$ に基づいて暗号化処理を行う。

- 25       さらに、メモリカード140中のメモリ1412においては、メモリカード130の場合に保持されていた公開暗号化鍵 $K_{Pp}$ の代わりに、公開復号鍵 $K_{Pma}$ が格納されている。したがって、復号処理部1460は、メモリ1412中に保持された公開復号鍵 $K_{Pma}$ に基づいて復号処理を行う。

メモリカード140のその他の部分は、実施例3のメモリカード130の構成

と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図14のメモ리카ード140内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内の鍵等の読出を不能化するためのモジュールTRMに組込まれる構成とすることも可能である。

[再生処理]

図15は、携帯電話機400内において、メモ리카ード140に保持された暗号化コンテンツデータから、音楽を再生して外部に出力するための再生処理を説明するフローチャートである。

10 図15を参照して、再生処理の説明を行なう。携帯電話機のキーボード1108等からのユーザの指示により、再生リクエストが与えられると（ステップS400）、携帯電話機400の[KPp, Crtf] KPma保持部1560からメモ리카ード140に対してデータ[KPp, Crtf] KPmaが出力される（ステップS402）。

15 メモ리카ード140においては、このデータ[KPp, Crtf] KPmaを復号部1460により復号し、公開暗号化鍵KPpと認証データCrtfとを獲得する（ステップS406）。コントローラ1420は、認証データCrtfに基づいて携帯電話機400の認証を行ない（ステップS406）、携帯電話機400が正規の機器であれば処理をステップS408に移行し、携帯電話機400が正規の機器でない場合、再生のための動作を行わずに処理を終了する（ステップS434）。

25 携帯電話機400が正規の機器である場合、コントローラ1420は、セッションキー発生部1450を制御してセッションキーKs2を発生させる（ステップS408）。コントローラ1420の制御により、このセッションキーKs2を暗号化処理部1452は公開暗号化鍵KPpにより暗号化して暗号化セッションキー[Ks2] Kpを生成し、この暗号化セッションキー[Ks2] Kpを、データバスBS3、端子1202およびメモリアンタフェース1200を介して、携帯電話機400に対して送信する（ステップS410）。

携帯電話機400では、カード140からの暗号化セッションキー[Ks2]

K<sub>p</sub>を受信すると、切換え回路1550を介して復号処理部1530が暗号化セッションキー[K<sub>s</sub>2] K<sub>p</sub>を受けて復号しセッションキーK<sub>s</sub>2を獲得する(ステップS412)。

5 携帯電話機400においては、セッションキー発生部1552においてセッションキーK<sub>s</sub>1を生成し(ステップS414)、暗号化処理部1554が、ステップS412において抽出されたセッションキーK<sub>s</sub>2により、セッションキーK<sub>s</sub>1を暗号化してデータ[K<sub>s</sub>1] K<sub>s</sub>2を生成し、データバスBS2を介して、カード140に対して送信する(ステップS416)。

10 メモリカード140は、携帯電話機400により生成され、かつ暗号化されたセッションキー[K<sub>s</sub>1] K<sub>s</sub>2を受け取り、復号処理部1454においてセッションキーK<sub>s</sub>2により復号し、セッションキーK<sub>s</sub>1を抽出する(ステップS418)。

続いて、メモリカード140は、メモリ1412から、暗号化されているデータ[K<sub>c</sub>] K<sub>p</sub>を読み出し(ステップS420)、暗号化処理部1456において、  
15 抽出したセッションキーK<sub>s</sub>1により、暗号化コンテンツキー[K<sub>c</sub>] K<sub>p</sub>を暗号化し、暗号化された暗号化コンテンツキー[[K<sub>c</sub>] K<sub>p</sub>] K<sub>s</sub>1をデータバスBS3等を介してデータバスBS2に与える(ステップS422)。

携帯電話機400の復号処理部1556は、メモリカード140から送信された暗号化された暗号化コンテンツキー[[K<sub>c</sub>] K<sub>p</sub>] K<sub>s</sub>1に対してセッションキーK<sub>s</sub>1により復号処理を行なうことにより、暗号化コンテンツキー[K<sub>c</sub>] K<sub>p</sub>を取得する(ステップS424)。  
20

さらに、携帯電話機400の復号処理部1530は、切換え回路1550を介して暗号化コンテンツキー[K<sub>c</sub>] K<sub>p</sub>を受け、K<sub>p</sub>保持部1540からのキーK<sub>p</sub>に基づいて、データ[K<sub>c</sub>] K<sub>p</sub>の復号処理を行なう(ステップS426)。

25 復号処理部1530が、復号処理によりコンテンツキーK<sub>c</sub>を抽出できた場合は(ステップS428)、処理は次のステップS430に進み、抽出できない場合は(ステップS428)、処理は終了する(ステップS434)。

復号処理部1530が復号処理により、コンテンツキーK<sub>c</sub>を抽出できた場合は、メモリカード140は、暗号化コンテンツデータ[D<sub>c</sub>] K<sub>c</sub>をメモリ14

1 2 から読出し、データベース B S 3 等を介してデータベース B S 2 に与える（ステップ S 4 3 0）。

携帯電話機 4 0 0 の復号処理部 1 5 2 0 は、暗号化コンテンツデータ [D c]  
K c を、抽出されたコンテンツキー K c により復号処理して平文の音楽データ D  
c を生成し、音楽再生部 1 5 0 8 は、コンテンツデータ D c を再生して混合部 1  
5 1 0 に与える。デジタルアナログ変換部 1 5 1 2 は、混合部 1 5 1 0 からのデ  
ータを受け取って変換し、外部に再生された音楽を出力し（ステップ S 4 3 2）、  
処理が終了する（ステップ S 4 3 4）。

このような構成とすることで、実施例 3 の携帯電話機 3 0 0 およびメモリカー  
ド 1 3 0 の奏する効果に加えて、携帯電話機 4 0 0 からのデータ [K P p, C r  
t f] K P m a に基づいて、メモリカード 1 4 0 が認証の結果、正規の機器と判  
断された携帯電話機 4 0 0 とメモリカード 1 4 0 の間でしか再生動作が行なわれ  
ないため、システムのセキュリティの向上と、著作権者の著作権の保護を図るこ  
とが可能となる。

#### [実施例 5]

図 1 6 は、本発明の実施例 5 の携帯電話機 5 0 0 の構成を説明するための概略  
ブロック図であり、実施例 4 の図 1 2 と対比される図である。

図 1 6 に示した実施例 5 の携帯電話機 5 0 0 の構成と、実施例 4 の携帯電話機  
4 0 0 の構成が異なる点は、以下のとおりである。

すなわち、図 1 6 においては、メモリカード 1 4 0 に代わりメモリカード 1 5  
0 が装着されており、さらに、メモリカード 1 5 0 から携帯電話機 5 0 0 に対し  
てコンテンツキー K c を送信する場合は、セッションキー K s 1 により暗号化さ  
れたデータ [K c] K s 1 として送信される。したがって、実施例 4 の場合のよ  
うに、コンテンツキー K c の送信の際に、キー K P p とキー K s 1 により 2 重に  
暗号化されているわけではないため、キー K s 1 による復号処理とキー K p によ  
る復号処理とは、独立に行なうことが可能となり、図 1 6 に示した携帯電話機 5  
0 0 においてはにおいては切換スイッチ 1 5 5 0 が省略されている。

すなわち、携帯電話機 5 0 0 の音楽再生モジュール 1 5 0 0 は、秘密復号鍵 K  
p を保持するための K p 保持部 1 5 4 0 と、メモリカード 1 5 0 からデータバス

Bs 2を介して与えられるデータ [Ks 2] KpをキーKpにより復号化するための復号処理部1530と、メモリカード150と携帯電話機の他の部分とのデータ授受にあたり、データバスBS 2上においてやり取りされるデータを暗号化するためのセッションキーKs 1を乱数等により発生するセッションキー発生部1552と、セッションキー発生部1552により生成されたセッションキーKs 1をメモリカード150からのセッションキーKs 2で暗号化して、データバスBS 2に与えるための暗号化処理部1554と、データバスBS 2によりメモリカード150から伝送され、セッションキーKs 1により暗号化コンテンツキーKcをセッションキーKs 1について復号して出力する復号処理部1556と、  
5 復号処理部1556から出力されるコンテンツキーKcに基づいて、データバスBs 2を介してメモリカード150から与えられる暗号化コンテンツデータ [Dc] Kcを復号して音楽再生部1508に与えるための復号処理部1520と、メモリカード150と携帯電話の他の部分とのデータ授受にあたり、携帯電話機500に対する認証機能を実現するために、再生装置である携帯電話機500の  
10 クラス（種類等）に固有な公開暗号鍵KPpと認証データCrtfとを、システムに共通な公開復号鍵KPmaにより暗号化して保持する [KPp、Crtf] KPma保持部1560とを備える。

携帯電話機500のその他の部分は、実施例4の携帯電話機400の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

20 なお、図16においても、説明の簡素化のため本発明のコンテンツデータの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

また、図16に示した構成においても、音楽再生部1508、Kp保持部1540、復号処理部1530、復号処理部1520、復号処理部1556、暗号化  
25 処理部1554、セッションキー発生部1552および [KPp、Crtf] KPma保持部1560を、TRMに組み込む構成とすることが可能である。

このような構成とすることで、すくなくとも、認証データ、復号鍵および平文化されたデータを外部から変更あるいは参照できないため、携帯電話機500の暗号化方式および秘密復号鍵を外部から不正に取得することが困難となり、セキ

セキュリティが向上する。

さらに、図16において実線で囲んだ領域に相当する音楽再生モジュール1500を、TRMとすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するコンテンツデータの最終的なデジタルデータについても、保護することが可能である。

#### [メモ리카ードの構成]

図17は、図16に示したメモ리카ード150の構成を説明するための概略ブロック図である。

メモ리카ード150の構成が、実施例4のメモ리카ード140の構成と異なる点は、コンテンツキーKcがメモリ1412中に暗号化されることなく、平分データとして格納されている点である。

メモ리카ード150のその他の部分は、実施例4のメモ리카ード140の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図17のメモ리카ード150内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組み込まれる構成とする。

#### [再生処理]

図18は、携帯電話機500内において、メモ리카ード150に保持された暗号化コンテンツデータから、音楽情報を復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

図18を参照して、再生処理についての説明を行なう。携帯電話機のキーボード1108等からのユーザの指示により、再生リクエストが与えられると（ステップS500）、携帯電話機500の[KPp, Crtf] KPma保持部1560からメモ리카ード150に対してデータ[KPp, Crtf] KPmaが出力される（ステップS502）。

メモ리카ード150においては、このデータ[KPp, Crtf] KPmaを復号部1460により復号し、公開暗号化鍵KPpと認証データCrtfとを獲得する（ステップS506）。コントローラ1420は、認証データCrtfに



基づいて携帯電話機500の認証を行ない（ステップS506）、携帯電話機500が正規の機器であれば処理をステップS508に移行し、携帯電話機500が正規の機器でない場合、再生のための動作を行わずに処理を終了する（ステップS534）。

- 5      携帯電話機500が正規の機器である場合、コントローラ1420は、セッションキー発生部1450を制御してセッションキーKs2を発生させる（ステップS508）。コントローラ1420の制御により、このセッションキーKs2を暗号化処理部1452は公開暗号化鍵Kpにより暗号化して暗号化セッションキー[Ks2]Kpを生成し、この暗号化セッションキー[Ks2]Kpを、
- 10     データバスBS3、端子1202およびメモリアンタフェース1200を介して、携帯電話機500に対して送信する（ステップS510）。

- 携帯電話機500では、カード150からの暗号化セッションキー[Ks2]Kpを受信すると、切換え回路1550を介して復号処理部1530が暗号化セッションキー[Ks2]Kpを受けて復号しセッションキーKs2を獲得する
- 15     （ステップS512）。

- 携帯電話機500においては、セッションキー発生部1552においてセッションキーKs1を生成し（ステップS514）、暗号化処理部1554が、ステップS512において抽出されたセッションキーKs2により、セッションキーKs1を暗号化してデータ[Ks1]Ks2を生成し、データバスBS2を介して、カード150に対して送信する（ステップS516）。
- 20

メモ리카ード150は、携帯電話機500により生成され、かつ暗号化されたセッションキー[Ks1]Ks2を受け取り、復号処理部1454においてセッションキーKs2により復号し、セッションキーKs1を抽出する（ステップS518）。

- 25     続いて、メモ리카ード150は、メモリ1412から、コンテンツキーKcを読み出す（ステップS520）。

続いて、メモ리카ード150は、暗号化処理部1456において、抽出したセッションキーKs1により、コンテンツキーKcを暗号化し、暗号化コンテンツキー[Kc]Ks1をデータバスBS3等を介してデータバスBS2に与える

(ステップS 5 2 2)。

携帯電話機500の復号処理部1556は、メモ리카ード150から送信された暗号化された暗号化コンテンツキー[Kc] Ks1に対して、セッションキーKs1により復号処理を行なうことにより、コンテンツキーKcを取得する(ステップS 5 2 4)。

メモ리카ード150は、暗号化コンテンツデータ[Dc] Kcをメモリ1412から読出し、データバスBS3等を介してデータバスBS2に与える(ステップS 5 3 0)。

携帯電話機500の復号処理部1520は、暗号化コンテンツデータ[Dc] Kcを、抽出されたコンテンツキーKcにより復号処理して平文のコンテンツデータDcを生成し、音楽再生部1508は、コンテンツデータDcを再生して混合部1510に与える。デジタルアナログ変換部1512は、混合部1510からのデータを受け取ってアナログ信号に変換し、外部に再生された音楽を出力し(ステップS 5 3 2)、処理が終了する(ステップS 5 3 4)。

このような構成とすることで、実施例4の携帯電話機400およびメモ리카ード130の奏する効果と同様に、携帯電話機500からのデータ[KPp, Crif] KPmaに基づいて、メモ리카ード150が認証の結果、正規の機器と判断された携帯電話機500とメモ리카ード150の間でしか再生動作が行なわれないため、著作権者の著作権の保護を図ることが、より簡易な構成で可能となる。

#### [実施例6]

図19は、本発明の実施例6の携帯電話機600の構成を説明するための概略ブロック図であり、実施例5の図16と対比される図である。

図19に示した実施例6の携帯電話機600の構成と、実施例5の携帯電話機500の構成が異なる点は、以下のとおりである。

すなわち、図19においては、携帯電話機600は、システム共通の秘密復号鍵Kcomを保持するためのKcom保持部1570と、復号処理部1556の出力を受けて、秘密復号鍵Kcomにより復号してコンテンツキーKcを獲得し、復号処理部1520に与える復号処理部1572をさらに備える構成となっている。

すなわち、実施例 5 においては、メモリカード 150 から携帯電話機 500 に対してコンテンツキー  $K_c$  を送信する場合は、セッションキー  $K_{s1}$  により暗号化されたコンテンツキー  $[K_c] K_{s1}$  として送信されたのに対し、実施例 6 においては、メモリカード 160 から携帯電話機 600 に対してコンテンツキー  $K_c$  を送信する場合は、秘密復号鍵  $K_{com}$  およびセッションキー  $K_{s1}$  により復号可能なように暗号化されたコンテンツキー  $[[K_c] K_{com}] K_{s1}$  として送信される。

携帯電話機 600 のその他の部分は、実施例 5 の携帯電話機 500 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図 19 においても、説明の簡素化のため本発明の音楽データの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

また、図 19 に示した構成において、音楽再生部 1508、 $K_p$  保持部 1540、復号処理部 1530、復号処理部 1520、復号処理部 1556、暗号化処理部 1554、セッションキー発生部 1552、 $[K_{pp}, C_{rtf}] K_{Pma}$  保持部 1560、 $K_{com}$  保持部および復号処理部 1572 を、TRM に組み込む構成とすることが可能である。

このような構成とすることで、すくなくとも、認証データ、復号鍵および平文化されたコンテンツデータを外部から不正に取得することができなくなり、セキュリティが向上する。

さらに、図 19 において実線で囲んだ領域に相当する音楽再生モジュール 1500 を、TRM とすることも可能である。このような構成とすれば、音楽データ等の著作権の存在するデータの最終的なデジタルデータについても、保護することが可能である。

#### [暗号／復号鍵の構成]

図 20 は、図 19 に示した携帯電話機 600 において使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

まず、図 19 に示した構成において、メモリカード 160 内のデータ処理を管理するための鍵としては、システムに共通な公開復号鍵  $K_{Pma}$  と、メモリカー

ド160が生成し各セッションに固有なセッションキーKs2とがある。

さらに、メモ리카ード外でのデータの授受における秘密保持のための暗号鍵としては、音楽再生モジュールの管理の鍵として、携帯電話機という再生装置のクラスに固有な公開暗号化鍵であって、鍵KPmaにより暗号化された形で携帯電話機600中の[KPp、Cr tf] KPma保持部1560に格納されている公開暗号鍵KPpと、このキーKPpで暗号化されたデータを復号化でき、キーKPpとは非対称な秘密復号鍵Kpと、システムに共通な秘密復号鍵Kcomと、各アクセスごとにセッションキー発生器1552において生成される共通鍵であるセッションキーKs1とが用いられる。

10 セッションキーKs1も各通信セッションに固有の値を有することになり、音楽再生モジュール1500において管理される。

さらに、メモ리카ード160に記録される著作物データについては、まず、音楽データ(コンテンツデータ)自体を暗号化するための共通鍵であるコンテンツキーKcがあり、この共通鍵Kcにより暗号化コンテンツデータが復号(平文化)されるものとする。

15 また、配信サーバ10から携帯電話機600に向けて、コンテンツキーKcが配信される場合には、このコンテンツキーKcは、すくなくとも秘密復号鍵Kcomにより復号可能なように暗号化されており、メモ리카ード160中には、この暗号化コンテンツキー[Kc] Kcomとして格納されているものとする。

20 さらに、著作権の存在するコンテンツデータDcは、このコンテンツデータをコンテンツキーKcで復号化可能な暗号化コンテンツデータ[Dc] Kcとしてメモ리카ード160に格納されているものとする。

[メモ리카ードの構成]

25 図21は、図19に示したメモ리카ード160の構成を説明するための概略ブロック図である。

メモ리카ード160の構成が、実施例5のメモ리카ード150の構成と異なる点は、コンテンツキーKcがメモリ1412中においては、暗号化データ[Kc] Kcomとして格納されている点である。

メモ리카ード160のその他の部分は、実施例5のメモ리카ード150の構成

と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

なお、図21のメモ리카ード160内も、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれる構成とすることも可能である。

[再生処理]

図22は、携帯電話機600内において、メモ리카ード160に保持された暗号化コンテンツデータから、音楽を再生して外部に出力するための再生処理を説明するフローチャートである。

図22を参照して、携帯電話機のキーボード1108等からのユーザの指示により、再生リクエストが与えられると(ステップS600)、携帯電話機600の[KPp, Crtf] KPma保持部1560からメモ리카ード160に対してデータ[KPp, Crtf] KPmaが出力される(ステップS602)。

メモ리카ード160においては、このデータ[KPp, Crtf] KPmaを復号部1460により復号し、公開暗号化鍵KPpと認証データCrtfとを獲得する(ステップS606)。コントローラ1420は、認証データCrtfに基づいて携帯電話機600の認証を行ない(ステップS606)、携帯電話機600が正規の機器であれば処理をステップS608に移行し、携帯電話機600が正規の機器でない場合、再生のための動作を行わずに処理を終了する(ステップS634)。

携帯電話機600が正規の機器である場合、コントローラ1420は、セッションキー発生部1450を制御してセッションキーKs2を発生させる(ステップS608)。コントローラ1420の制御により、このセッションキーKs2を暗号化処理部1452は公開暗号化鍵KPpにより暗号化して暗号化セッションキー[Ks2] Kpを生成し、この暗号化セッションキー[Ks2] Kpを、データバスBS3、端子1202およびメモリアンタフェース1200を介して、携帯電話機600に対して送信する(ステップS610)。

携帯電話機600では、カード160からの暗号化セッションキー[Ks2] Kpを受信すると、切換え回路1550を介して復号処理部1530が暗号化セ

セッションキー [K s 2] K p を受けて復号しセッションキー K s 2 を獲得する (ステップ S 6 1 2)。

5 携帯電話機 6 0 0 においては、セッションキー発生部 1 5 5 2 においてセッションキー K s 1 を生成し (ステップ S 6 1 4)、暗号化処理部 1 5 5 4 が、ステップ S 6 1 2 において抽出されたセッションキー K s 2 により、セッションキー K s 1 を暗号化して暗号化セッションキー [K s 1] K s 2 を生成し、データベース B S 2 を介して、カード 1 6 0 に対して送信する (ステップ S 6 1 6)。

10 メモリカード 1 6 0 は、携帯電話機 6 0 0 により生成された暗号化セッションキー [K s 1] K s 2 を受け取り、復号処理部 1 4 5 4 においてセッションキー K s 2 により復号し、セッションキー K s 1 を抽出する (ステップ S 6 1 8)。

続いて、メモリカード 1 6 0 は、メモリ 1 4 1 2 から、暗号化コンテンツキー [K c] K c o m を読出す (ステップ S 6 2 0)。

15 続いて、メモリカード 1 6 0 は、暗号化処理部 1 4 5 6 において、抽出したセッションキー K s 1 により、暗号化コンテンツキー [K c] K c o m を暗号化し、暗号化された暗号化コンテンツキー [[K c] K c o m] K s 1 をデータベース B S 3 等を介してデータベース B S 2 に与える (ステップ S 6 2 2)。

20 携帯電話機 6 0 0 の復号処理部 1 5 5 6 は、メモリカード 1 6 0 から送信された暗号化された暗号化コンテンツキー [[K c] K c o m] K s 1 に対してセッションキー K s 1 により復号処理を行なうことにより、暗号化コンテンツキー [K c] K c o m を取得する (ステップ S 6 2 4)。

さらに、携帯電話機 6 0 0 の復号処理部 1 5 7 2 は、復号処理部 1 5 5 6 から暗号化コンテンツキー [K c] K c o m を受け、K c o m 保持部 1 5 7 0 からのキー K c o m に基づいて、データ [K c] K c o m の復号処理を行なう (ステップ S 6 2 6)。

25 復号処理部 1 5 7 2 が、復号処理によりコンテンツキー K c を抽出できた場合は (ステップ S 6 2 8)、処理は次のステップ S 6 3 0 に進み、抽出できない場合は (ステップ S 6 2 8)、処理は終了する (ステップ S 6 3 4)。

復号処理部 1 5 7 2 が復号処理により、コンテンツキー K c を抽出できた場合は、メモリカード 1 6 0 は、暗号化コンテンツデータ [D c] K c をメモリ 1 4

12から読出し、データバスBS3等を介してデータバスBS2に与える（ステップS630）。

5 携帯電話機600の復号処理部1520は、暗号化コンテンツデータ[Dc]Kcを、抽出されたコンテンツキーKcにより復号処理して平文のコンテンツデータDcを生成し、音楽再生部1508は、コンテンツデータDcを再生して混合部1510に与える。デジタルアナログ変換部1512は、混合部1510からのデータを受け取って変換し、外部に再生された音楽を出力し（ステップS632）、処理が終了する（ステップS634）。

10 このような構成とすることで、実施例4の携帯電話機400およびメモ리카ード140の奏する効果と同様に、携帯電話機600からのデータ[KPp, Crtf]KPmaに基づいて、メモ리카ード160が認証の結果、正規の機器と判断された携帯電話機600とメモ리카ード160の間でしか再生動作が行なわれないため、システムのセキュリティの向上と、著作権者の著作権の保護を図ることが可能となる。

15 この発明を詳細に説明し示してきたが、これは例示のためのみであって、限定となつてはならず、発明の精神と範囲は添付の請求の範囲によってのみ限定されることが明らかに理解されるであろう。

## 請求の範囲

1. 暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置（100）であって、

- 5 前記暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号するためのコンテンツキーを暗号化した暗号化コンテンツキーを格納するためのデータ格納部（110、120、130）と、

前記データ格納部からの出力を受けて、前記暗号化コンテンツデータを再生するためのデータ再生部（1500）とを備え、

- 10 前記データ再生部は、

前記データ格納部から読み出された前記暗号化コンテンツキーを復号するための第1の復号鍵を保持する第1の鍵保持部（1540）と、

前記データ格納部からの前記暗号化コンテンツキーを基にして、前記第1の鍵保持部からの出力により復号処理を行なうことで、前記コンテンツキーを抽出する第1の復号処理部（1530）と、

- 15 前記データ格納部から読み出された前記暗号化コンテンツデータを受けて、前記第1の復号処理部の出力により復号してコンテンツデータを抽出するための第2の復号処理部（1520）とを含む、データ再生装置。

2. 前記データ再生部は、

- 20 前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスする毎に更新される第1のセッションキーを生成する第1のセッションキー発生部（1502）と、

前記第1のセッションキーを前記データ格納部にて復号可能な第1の暗号鍵で暗号化して前記データ格納部に与えるための第1の暗号化処理部（1504）と、

- 25 前記第1のセッションキーでさらに暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記第1のセッションキーについて復号して前記第1の復号処理部に与える第3の復号処理部（1506）をさらに含む、請求項1記載のデータ再生装置。

3. 前記コンテンツデータは、データ量を削減するための符号化方式にて符号化



された符号化音楽データであって、

前記データ再生部は、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音楽再生部（１５０８）と、

5 再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部（１５１２）とをさらに含む、請求項２に記載のデータ再生装置。

4. 前記データ再生部は、第三者には読出不可能なセキュリティ領域に設けられる、請求項３に記載のデータ再生装置。

5. 前記データ格納部（１２０）は、

10 前記データ格納部に与えられるデータを保持するための記憶部（１４１２）と、前記第１の暗号化鍵を保持する第２の鍵保持部（１４０１）と、

前記第１の暗号化鍵により暗号化されたデータを復号するための第２の復号鍵を保持するための第３の鍵保持部（１４０２）と、

15 前記第２の復号鍵に基づいて、前記データ再生部から前記第１の暗号化鍵により暗号化されて伝達された前記第１のセッションキーを復号するための第４の復号処理部（１４０４）と、

前記第４の復号処理部で抽出された前記第１のセッションキーにより、前記記憶部に保持されたデータを暗号化して出力するための第２の暗号化処理部（１４０６）とを備える、請求項２に記載のデータ再生装置。

20 6. 前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項５に記載のデータ再生装置。

7. 前記データ再生部は、前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスするごとに異なる第２のセッションキーを、さらに、前記第１の復号鍵により復号可能な暗号化を施して供給を受け、

25 前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツデータの取得のためにアクセスするごとに更新される第１のセッションキーを生成する第１のセッションキー発生部（１５５２）と、

前記第１のセッションキーを、外部から入力されたデータから前記第１の復号

鍵に基づいて前記第 1 の復号処理部にて抽出された前記第 2 のセッションキーで暗号化して前記データ格納部に与えるための第 2 の暗号処理部（1554）と、

前記第 1 のセッションキーでさらに暗号化された上で前記データ格納部から取得した前記暗号化コンテンツキーを、前記第 1 のセッションキーについて復号して前記第 1 の復号処理部に与える第 3 の復号処理部（1556）をさらに含む、請求項 1 記載のデータ再生装置。

8. 前記コンテンツデータは、データ量を削減するための符号化方式にて符号化された符号化音楽データであって、

前記データ再生部は、

前記符号化音楽データから前記符号化方式に基づいて音楽データを再生する音楽再生部と、

再生した前記音楽データをアナログ信号に変換するデジタルアナログ変換部とをさらに含む、請求項 7 に記載のデータ再生装置。

9. 前記データ再生部は、第三者には読出不可能なセキュリティ領域に設けられる、請求項 8 項に記載のデータ再生装置。

10. 前記データ格納部（130）は、

前記データ格納部に与えられるデータを保持するための記録部（1412）と、

前記暗号化コンテンツデータを取得のためにアクセスされるごとに更新する第 2 のセッションキーを発生する第 2 のセッションキー発生部（1450）と、

前記第 1 の復号鍵にて復号可能な第 2 の暗号化鍵により、暗号化処理を行なう第 3 の暗号化処理部（1452）と、

前記第 2 のセッションキーに基づいて、前記データ再生部から前記第 2 のセッションキーにて暗号化されて伝達された前記第 1 のセッションキーを復号するための第 5 の復号処理手段（1454）と、

前記第 5 の復号処理手段にて抽出された前記第 1 のセッションキーにより、前記記憶部に保持されたデータを暗号化して出力するための第 4 の暗号化処理部（1456）とを備える、請求項 7 記載のデータ再生装置。

11. 前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項 10 記載のデータ再生装置。

12. 前記データ再生部は、

少なくとも前記第1の鍵保持部と、前記第1の復号処理部と、前記第2の復号処理部とが、第三者には読出不可能なセキュリティ領域に設けられている、請求項1記載のデータ再生装置。

5 13. 暗号化コンテンツデータを復号してコンテンツデータの再生を行なうためのデータ再生装置であって、

前記暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号するためのコンテンツキーを保持し、かつ、前記データ再生装置に着脱可能なデータ格納部(140、150、160)と、

10 前記データ格納部からの出力を受けて、前記暗号化コンテンツデータを再生するためのデータ再生部(1500)とを備え、

前記データ再生部は、

前記データ格納部から読み出された前記暗号化コンテンツデータを受けて、復号してコンテンツデータを抽出するための第1の復号処理部(1520)と、

15 認証データを認証鍵により復号可能な暗号化を施して保持し前記データ格納部に対して出力可能な認証データ保持部(1560)とを含み、

前記データ格納部は、

前記認証鍵により暗号化されて前記データ再生部から与えられる前記認証データを復号して抽出するための第2の復号処理部(1460)と、

20 前記第2の復号処理部により抽出された前記認証データに基づいて認証処理を行う制御手段(1420)とを含む、データ再生装置。

14. 前記データ再生部は、

前記データ格納部に対して前記暗号化コンテンツキーの取得のためにアクセスする毎に更新される第1のセッションキーを生成するセッションキー発生部(1552)と、

25 前記セッションキーを前記データ格納部にて復号可能な第1の暗号鍵で暗号化して前記データ格納部に与えるための暗号化処理部(1554)と、

前記第1のセッションキーで暗号化されて前記データ格納部から受信した前記暗号化コンテンツキーを、前記第1のセッションキーについて復号する第3の復

号処理部（１５５６）とをさらに含む、請求項１３記載のデータ再生装置。

１５．前記第３の復号処理部は、復号結果を前記暗号化コンテンツデータを復号するためのコンテンツキーとして前記第１の復号処理部に与える、請求項１４記載のデータ再生装置。

- ５      １６．前記認証データ保持部は、第１の復号鍵で復号可能な暗号化を施すための第２の暗号鍵を前記認証データとともに前記認証鍵により復号可能な暗号化を施して保持し、前記データ格納部に対して出力し、

前記データ再生部は、前記第２の暗号鍵で暗号化された上で前記データ格納部から受信した前記第１の暗号化鍵を、前記第１の復号鍵にて復号し、前記暗号化  
１０      処理部に与える第４の復号処理部（１５３０）をさらに備える、請求項１４記載のデータ再生装置。

１７．前記第４の復号処理部（１５３０）は、さらに、

前記第１の復号鍵で復号可能なように前記第２の暗号鍵で暗号化され、さらに前記第１のセッションキーで暗号化された上で前記データ格納部から受信した前  
１５      記コンテンツキーを前記第３の復号処理部が前記第１のセッションキーについて復号した結果を入力として受けて、前記第２の暗号化鍵にて暗号化されたコンテンツキーを前記第１の復号鍵にて復号し、前記第１の復号処理部に与える、請求項１６記載のデータ再生装置。

１８．前記データ再生部は、

- ２０      予め定められた第２復号鍵にて復号するための第５の復号処理部（１５７２）をさらに備え、

前記第５の復号処理部は、

前記第２の復号鍵で復号可能な暗号化を施されて、さらに前記第１のセッションキーで暗号化された上で前記データ格納部から受信した前記コンテンツキーを  
２５      前記第３の復号部が前記第１のセッションキーについて復号した結果を入力として受け、前記第２の復号鍵にて復号し、前記第１の復号処理部に与える、請求項１４記載のデータ再生装置。

１９．前記データ格納部は、前記データ再生部に対して着脱可能なメモリカードである、請求項１３項に記載のデータ再生装置。

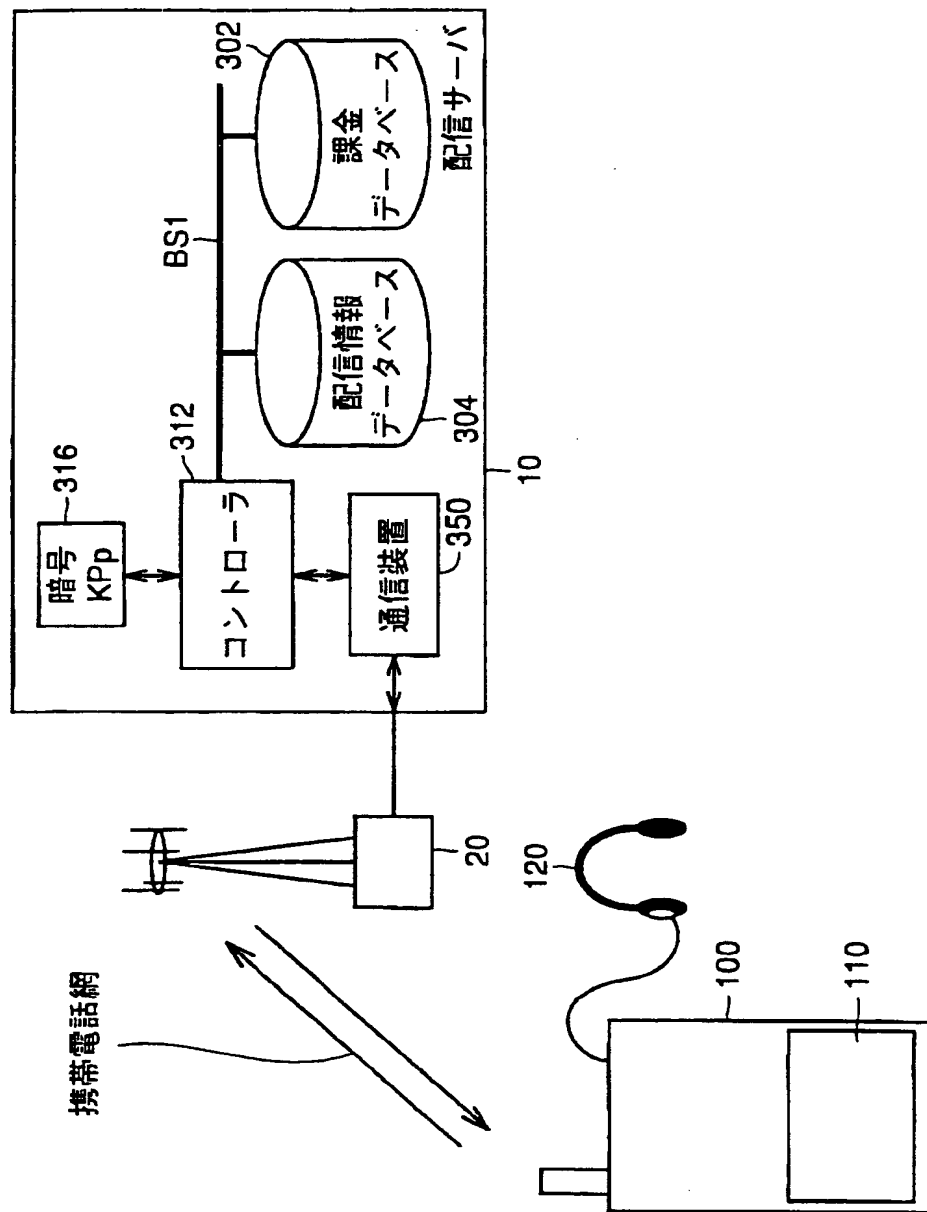
20. 前記データ再生装置は、さらに、簡易携帯電話網を含む携帯電話網に接続するインタフェースを備える、請求項13に記載のデータ再生装置。

21. 前記データ再生装置は、さらに、前記インタフェースを介して通話を行なう通話処理部を備える、請求項20に記載のデータ再生装置。

5 22. 前記データ格納部は、前記データ再生部に対して着脱可能である、請求項21に記載のデータ再生装置。

This Page Blank (uspto)

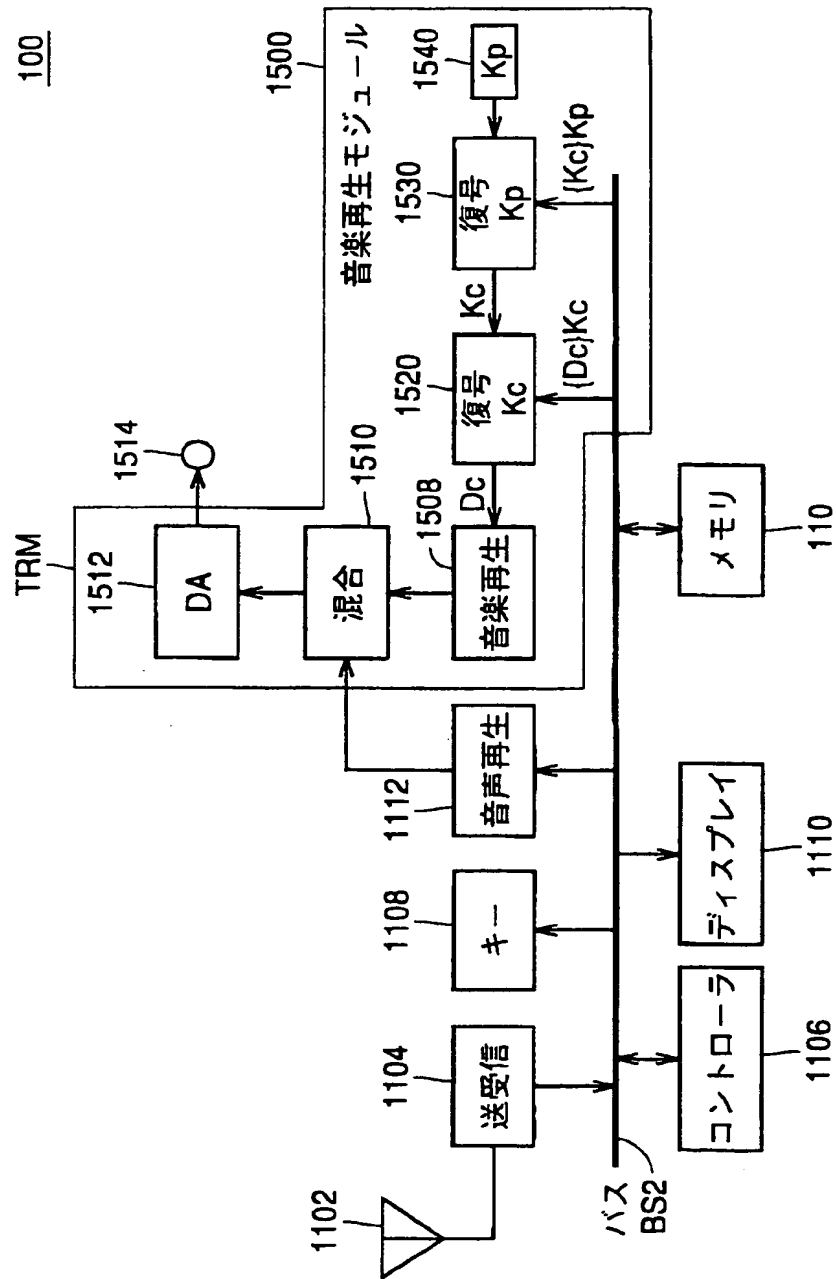
FIG. 1



This Page Blank (uspto)

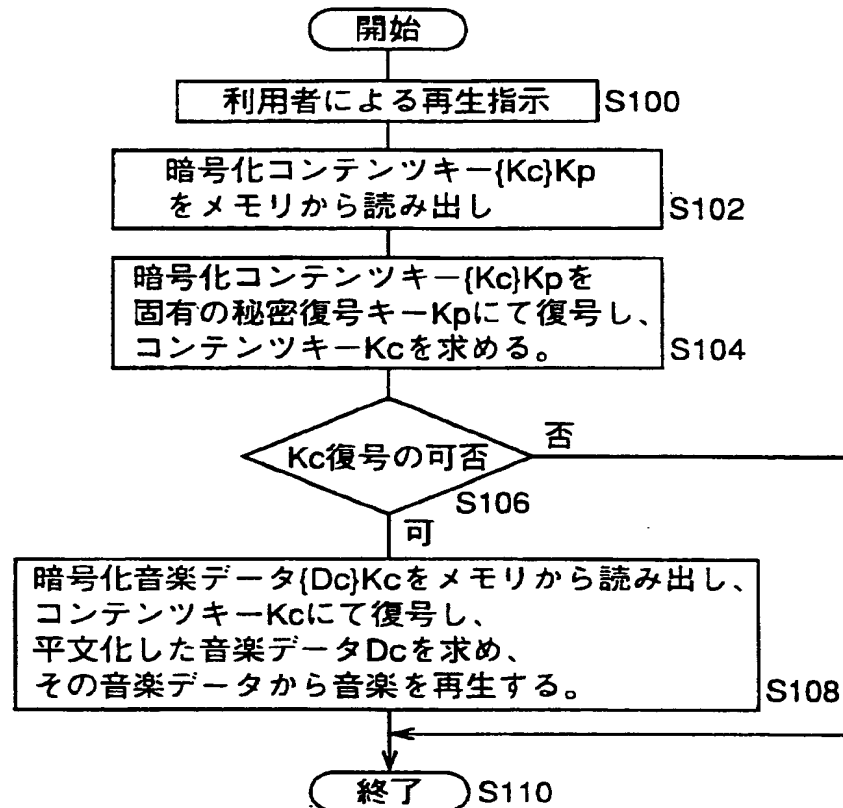


FIG. 2



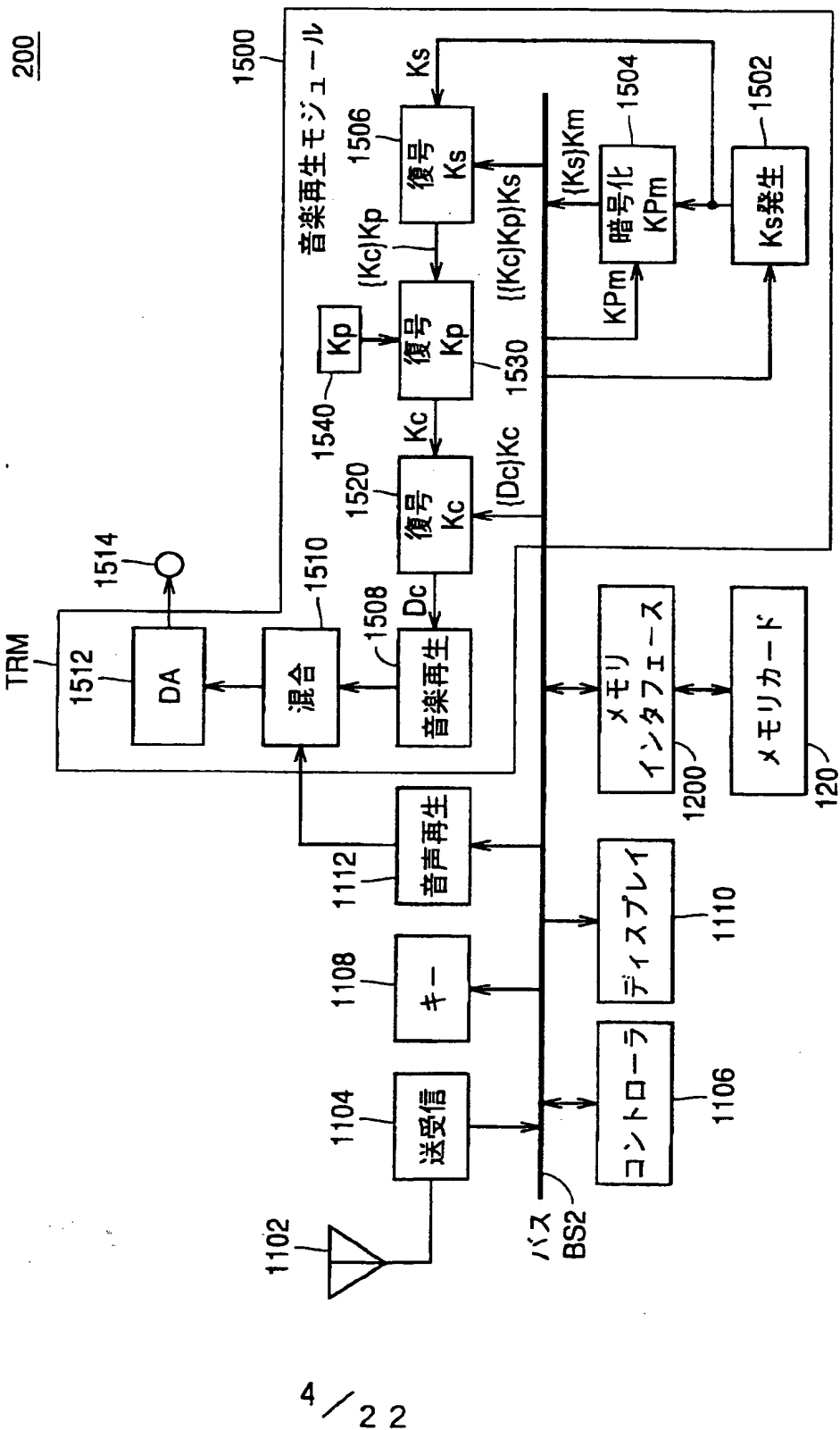
This Page Blank (uspto)

FIG. 3



This Page Blank (uspto)

FIG. 4



This Page Blank (uspto)

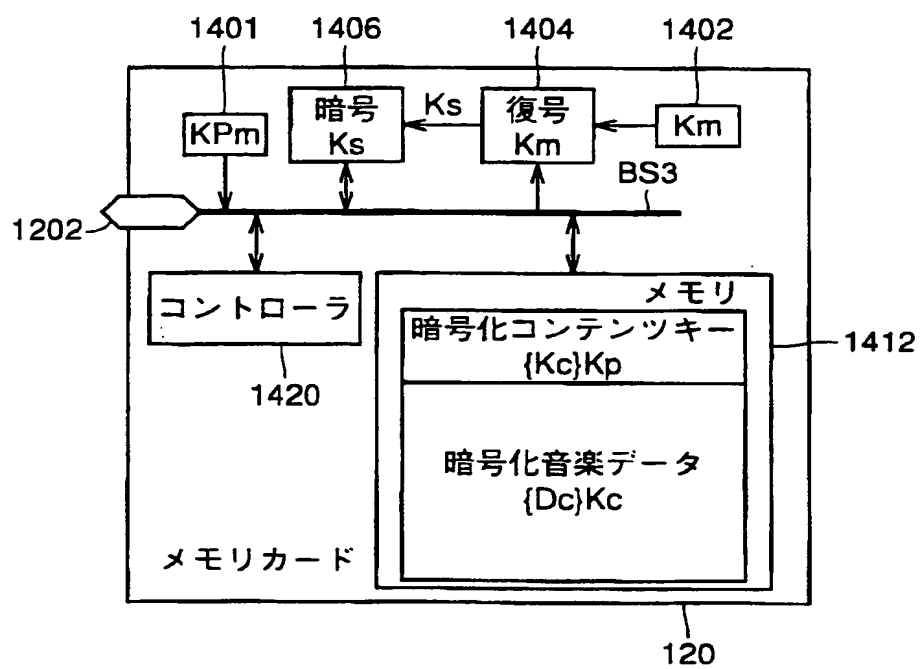
FIG. 5

	記号	属性	特性
メモリカード 管理の鍵	Km	秘密復号鍵	メモリカード毎に異なる
	KPm	公開暗号鍵	KPmで暗号化されたデータは非対称な 復号鍵Kmで復号可能
音楽再生モジュール 管理の鍵	Kp	秘密復号鍵	データ再生装置毎に異なる
	Ks	共通鍵	データ再生装置 (携帯電話機) 固有 セッション固有
配信データ	KPp	公開暗号鍵	メモリと音楽再生モジュール間 のアクセス毎に発生
	Kc	共通鍵	KPpで暗号化されたデータは非対称な 復号鍵Kpで復号可能
	Dc	コンテンツ データ	暗号化コンテンツデータの復号鍵 例：音楽データ

This Page Blank (uspto)

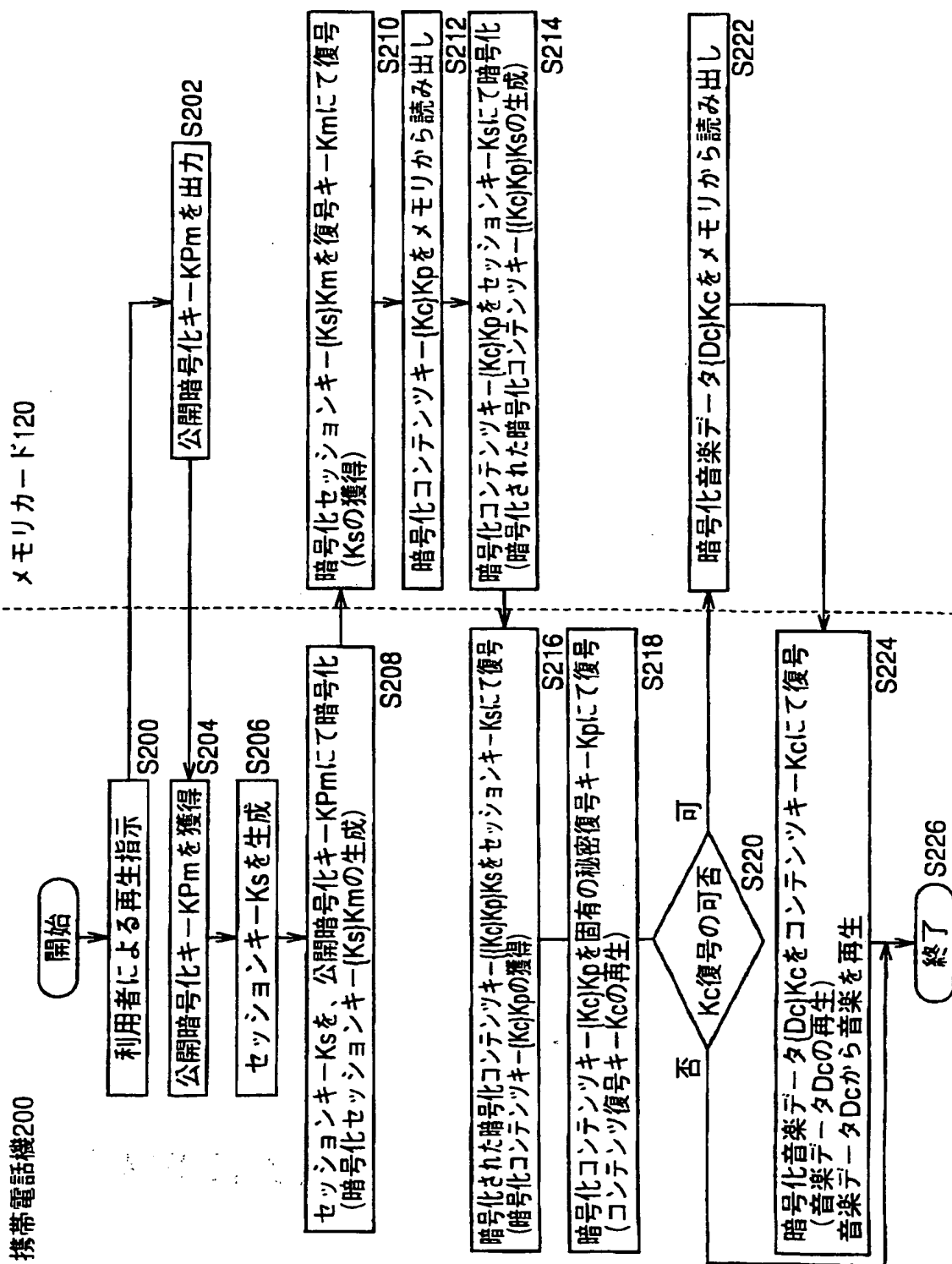


FIG. 6



This Page Blank (uspto)

FIG. 7



This Page Blank (uspto)



This Page Blank (uspto)

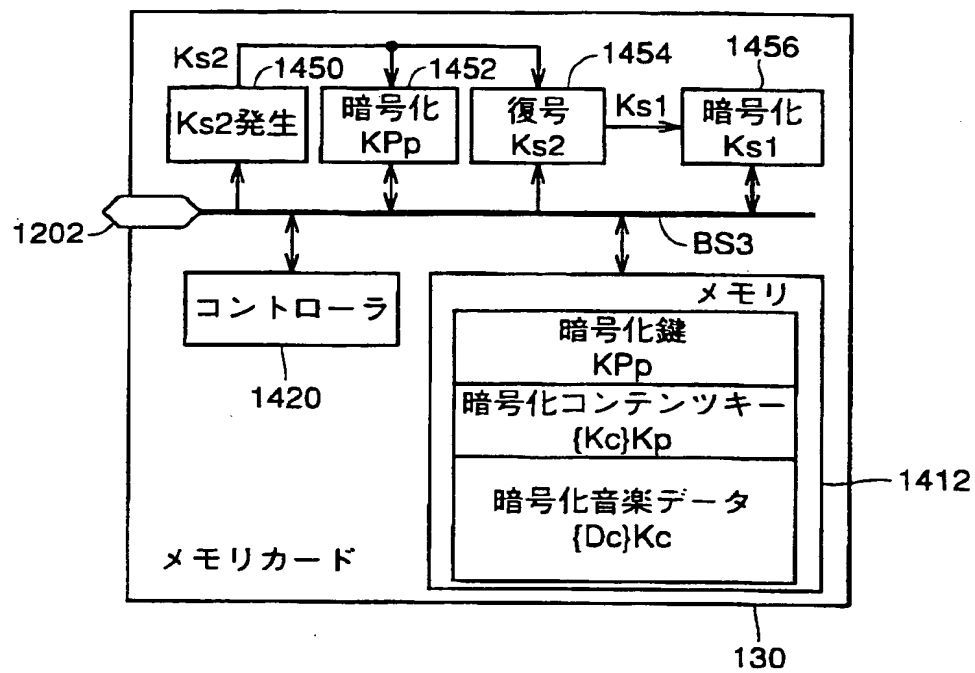
FIG. 9

	記号	属性	特性
メモリカード 管理の鍵	Km	秘密復号鍵	メモリカード毎に異なる
	KPm	公開暗号鍵	KPmで暗号化されたデータは非対称な 復号鍵Kmで復号可能
	Ks2	共通鍵	メモリと音楽再生モジュール間 のアクセス毎に発生
	Kp	秘密復号鍵	データ再生装置毎に異なる
音楽再生モジュール 管理の鍵	Ks1	共通鍵	メモリと音楽再生モジュール間 のアクセス毎に発生
	KPp	公開暗号鍵	KPpで暗号化されたデータは非対称な 復号鍵Kpで復号可能
配信データ	Kc	共通鍵	暗号化コンテンツデータの復号鍵
	Dc	コンテンツ データ	例：音楽データ

**This Page Blank (uspto)**

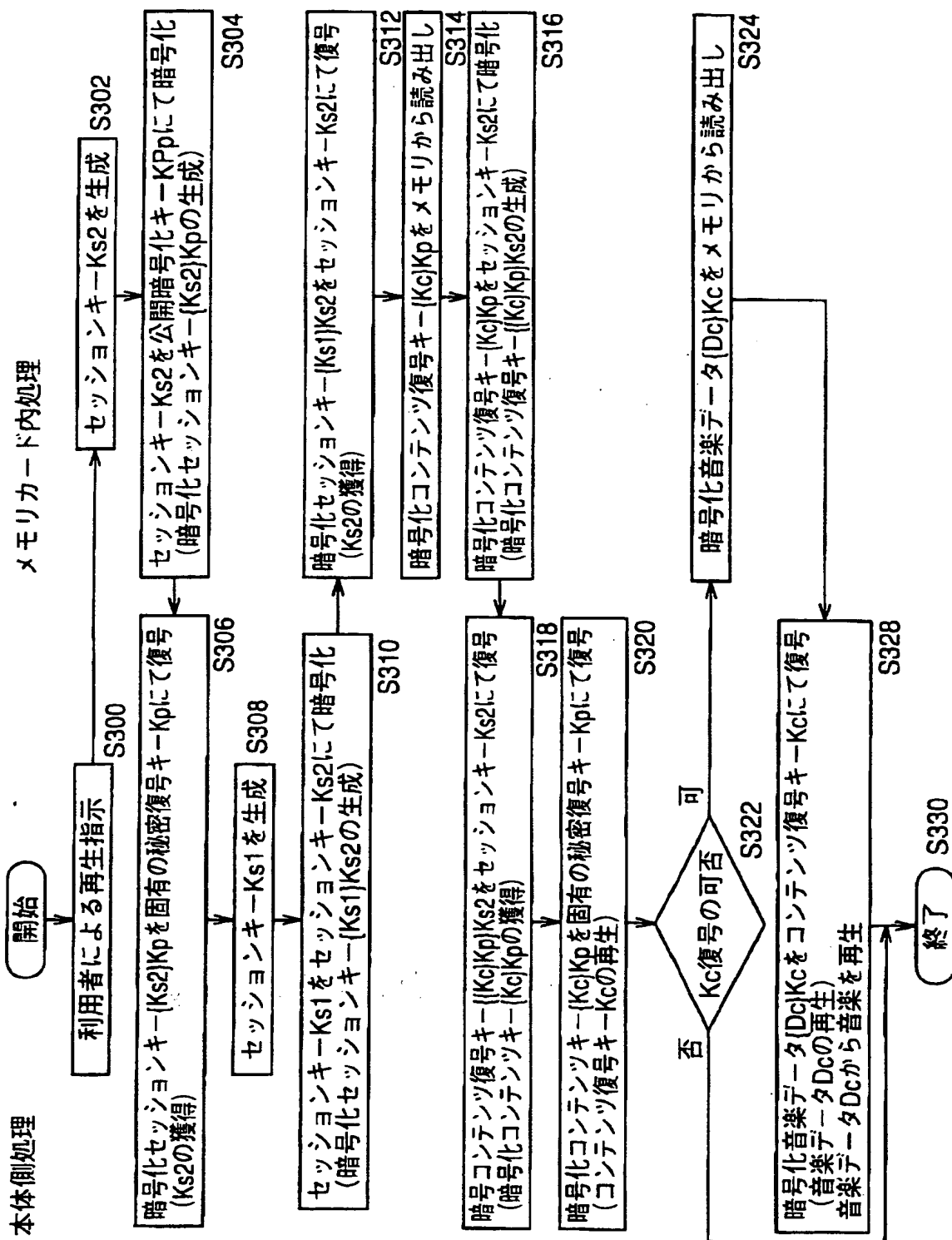


FIG. 10



This Page Blank (uspto)

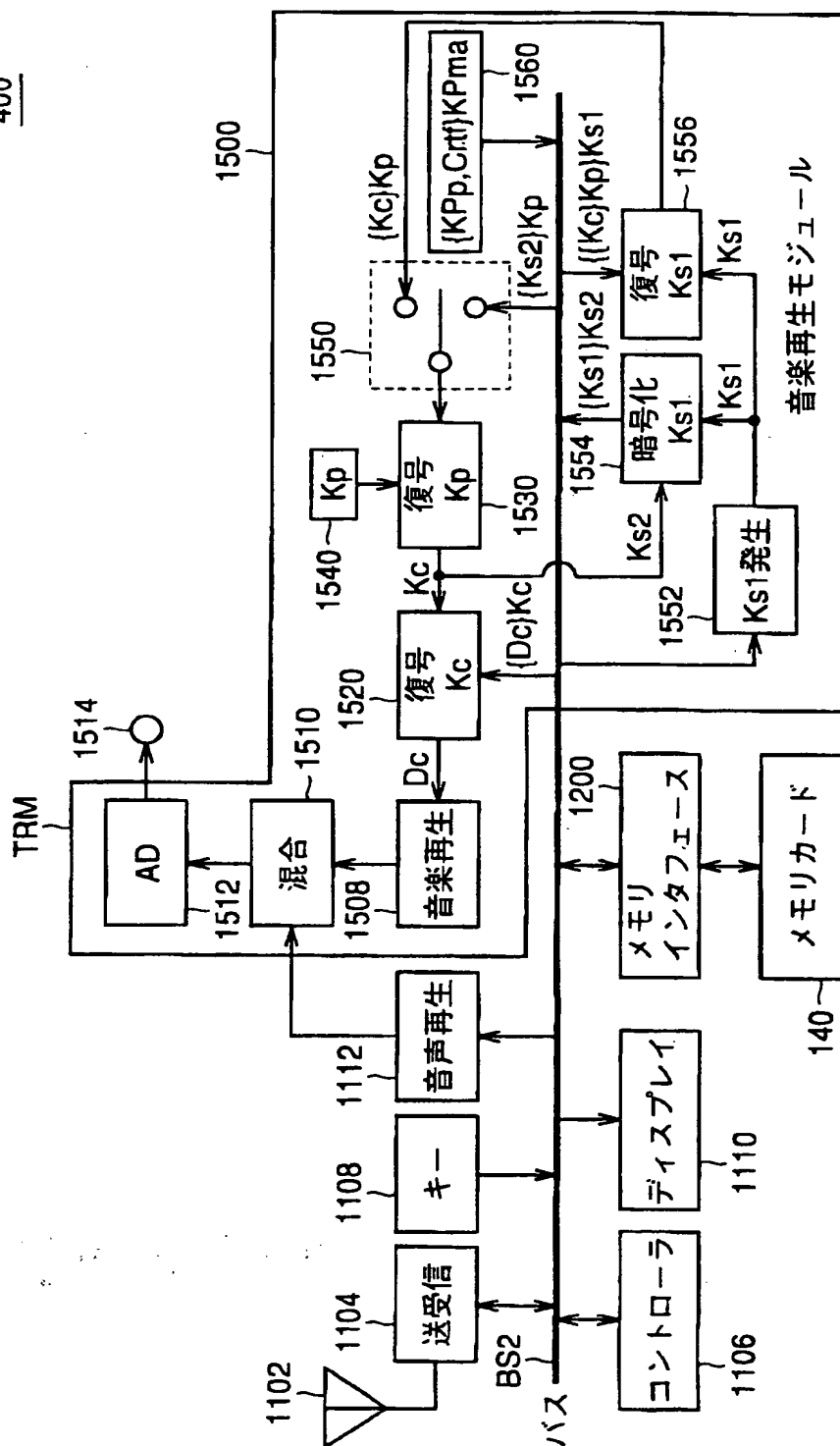
FIG. 11



This Page Blank (uspto)

FIG. 12

400



**This Page Blank (uspto)**

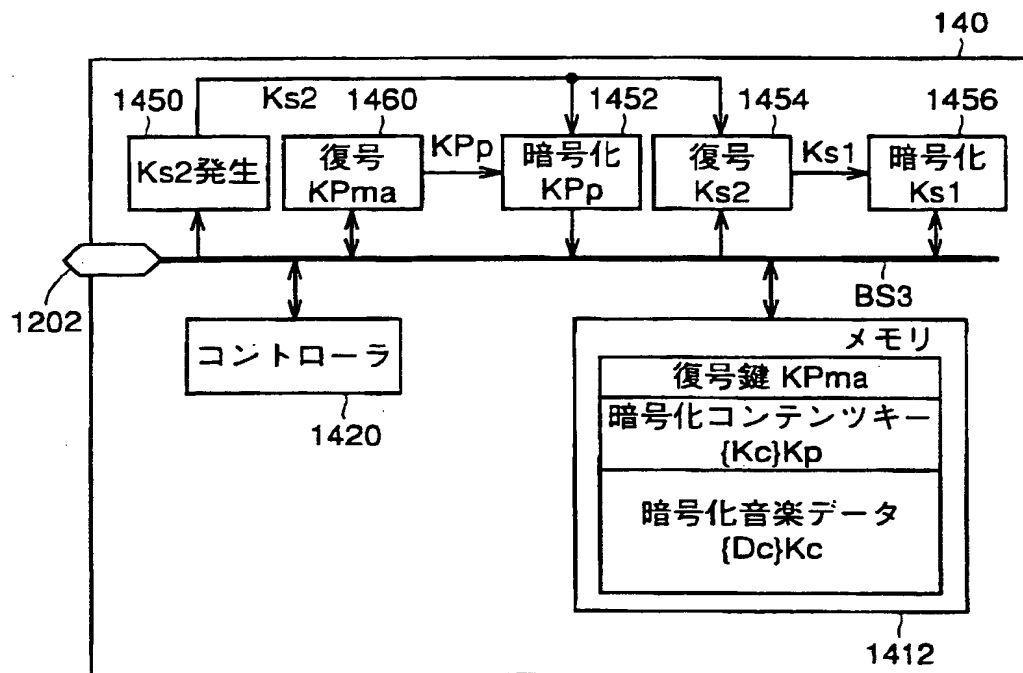
FIG. 13

	記号	属性	特性	
メモリカード 管理の鍵	KPma	公開復号鍵	システム共通	(KPp, Cpf)KPmaの復号によってKPpの認証を行う機能を有する 認証鍵
	Ks2	共通鍵	セッションキー	メモリカードと音楽生成モジュール艦のアクセス毎に発生
音楽生成 モジュール 管理の鍵	KPp	公開暗号鍵	再生装置のクラス (種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる 非対称な秘密復号鍵Kpにて復号可能
	Kp	秘密復号鍵	再生装置のクラス (種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる 非対称な公開暗号鍵KPpにて暗号化した暗号データを平分化
	Ks1	共通鍵	セッション固有	メモリカードと音楽生成モジュール艦のアクセス毎に発生
配信データ	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
	Dc	データ	コンテンツデータ	例：音楽データ

This Page Blank (uspto)

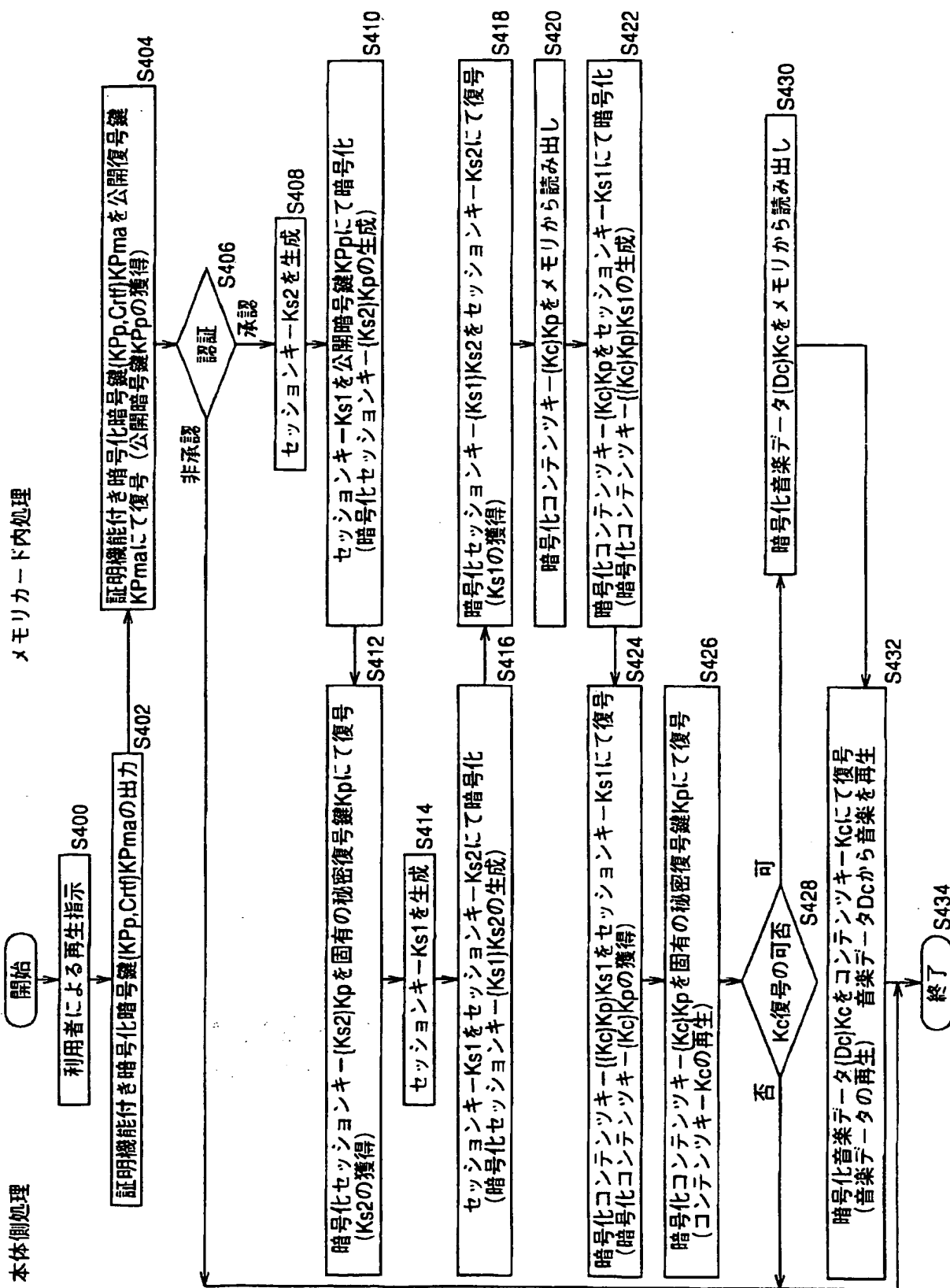


FIG. 14



This Page Blank (uspto)

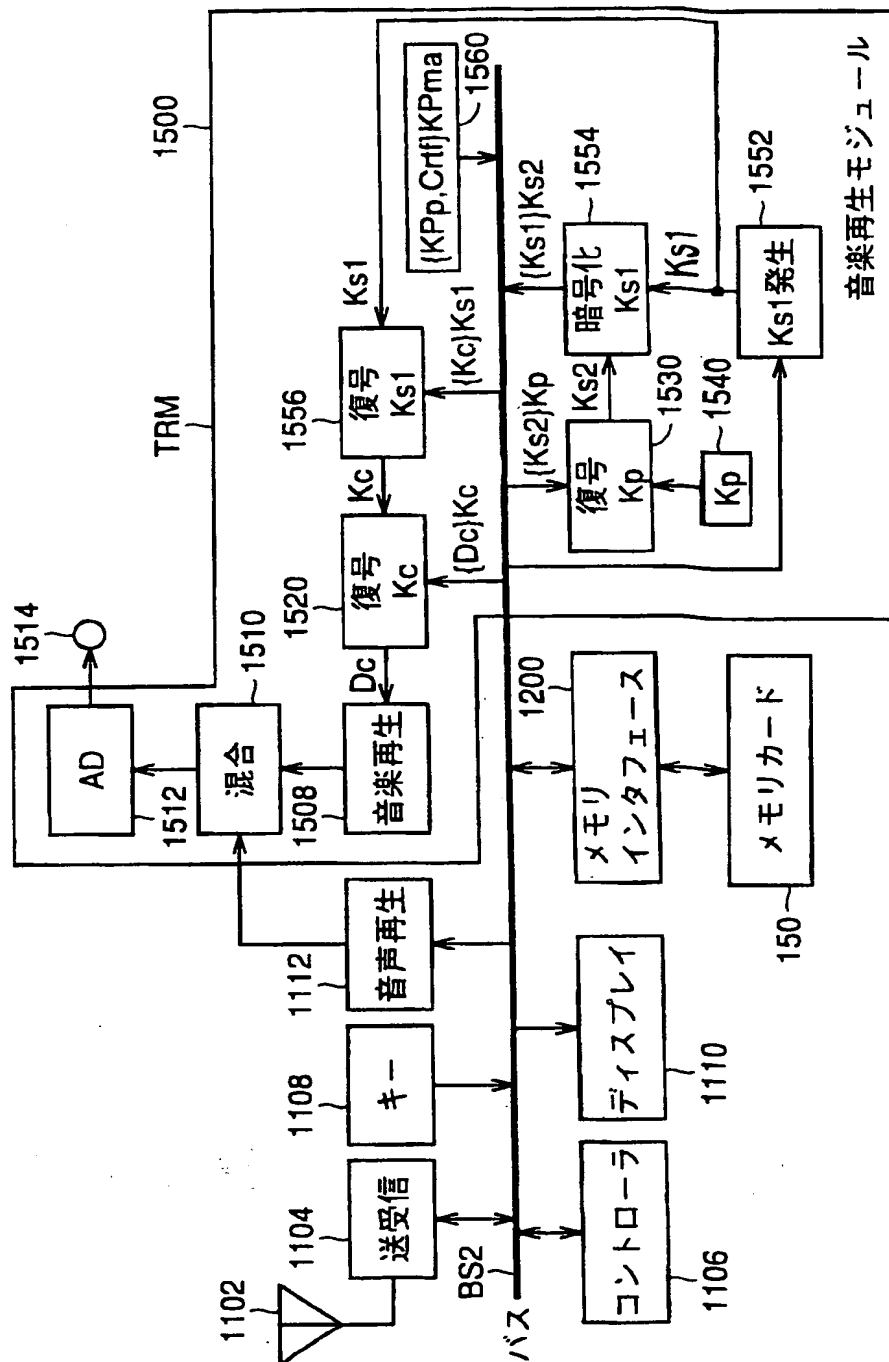
FIG. 15



**This Page Blank (uspto)**

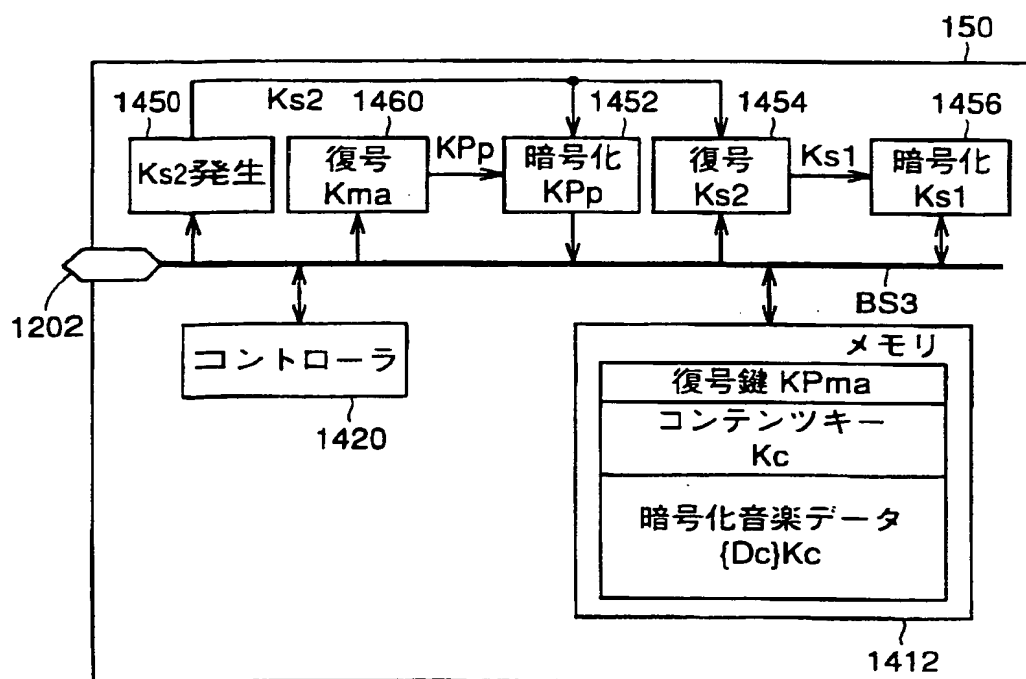
FIG. 16

500



**This Page Blank (uspto)**

FIG. 17



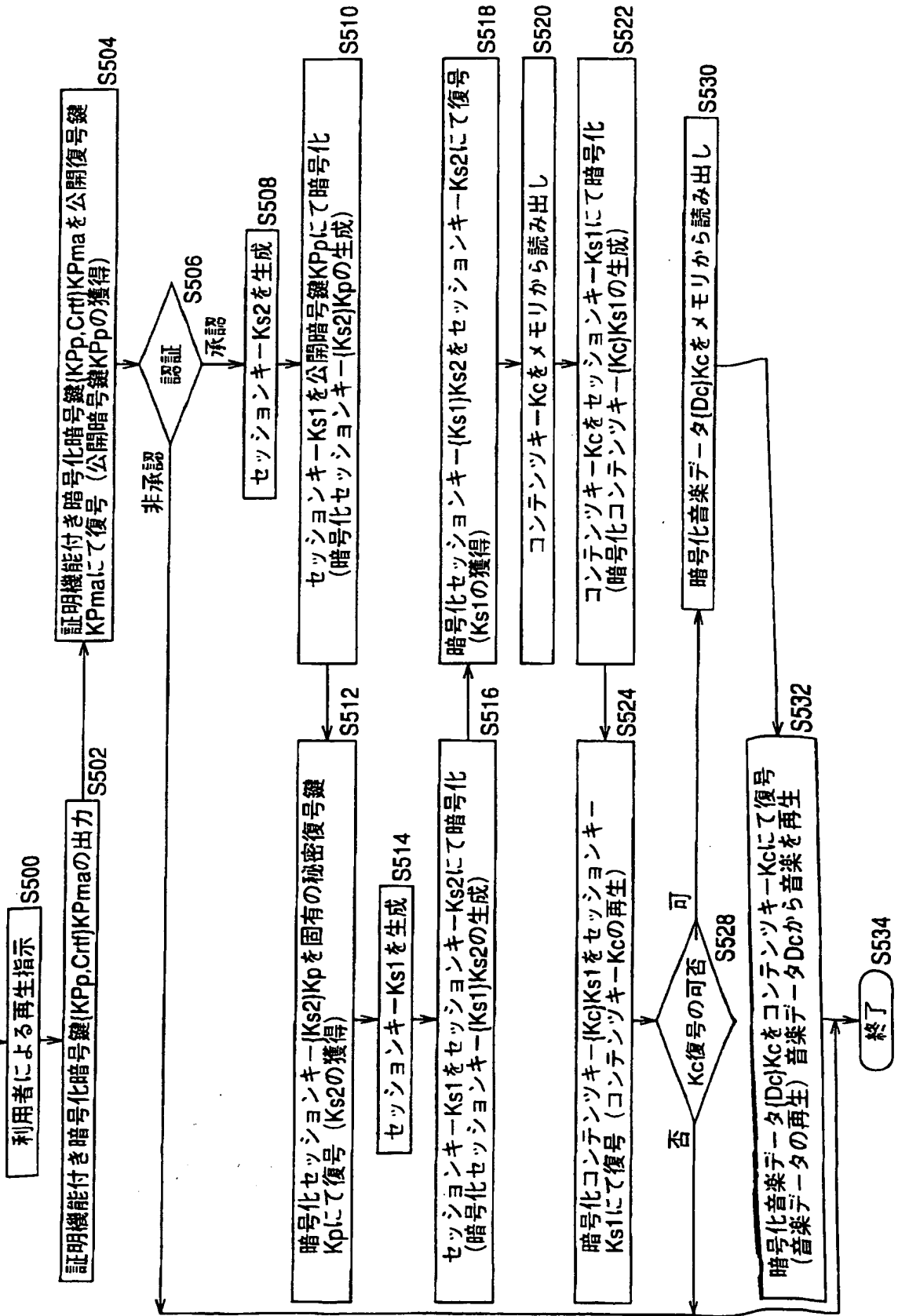
This Page Blank (uspto)



FIG. 18

本体側処理

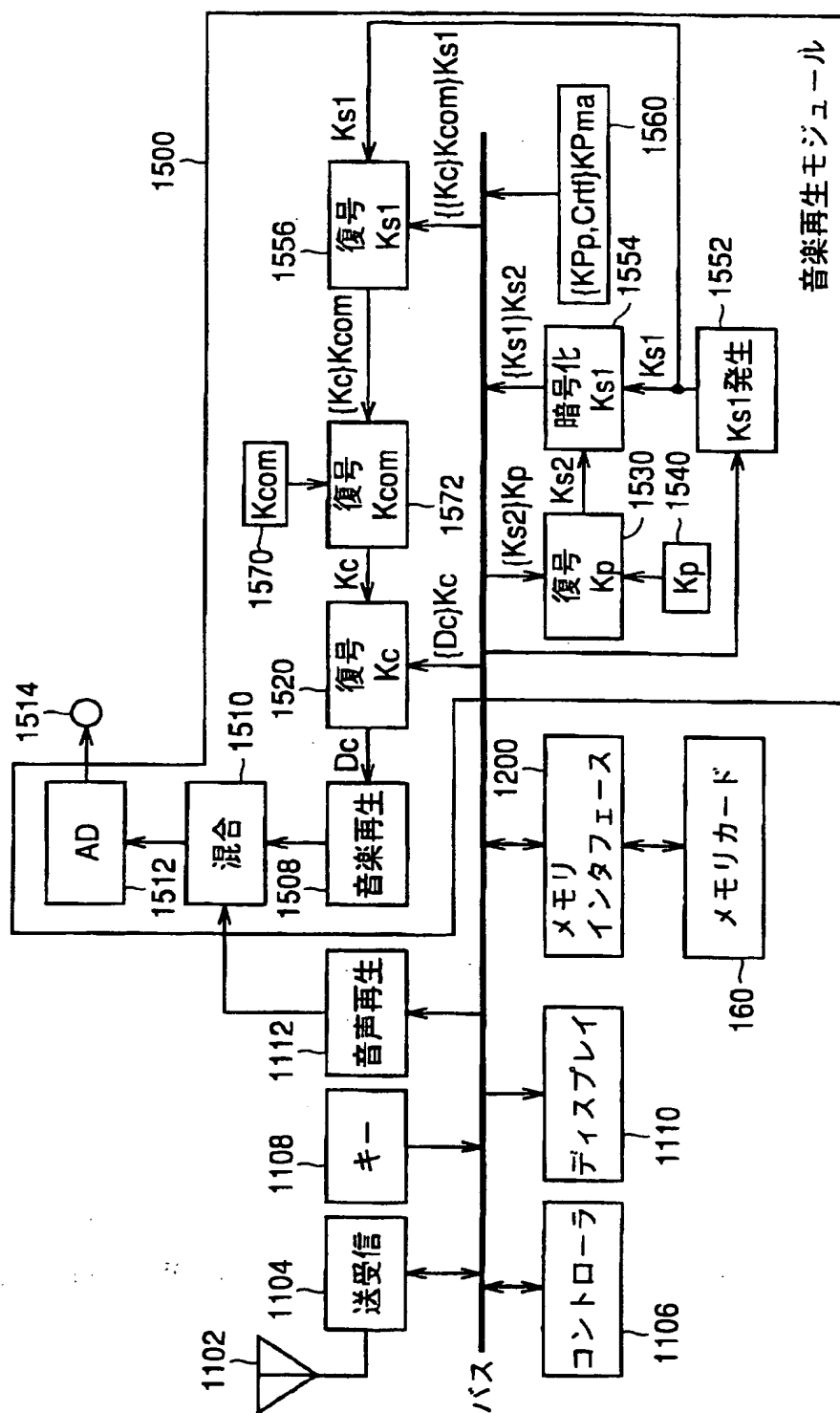
メモリカード内処理



This Page Blank (uspto)

FIG. 19

600



19 / 22

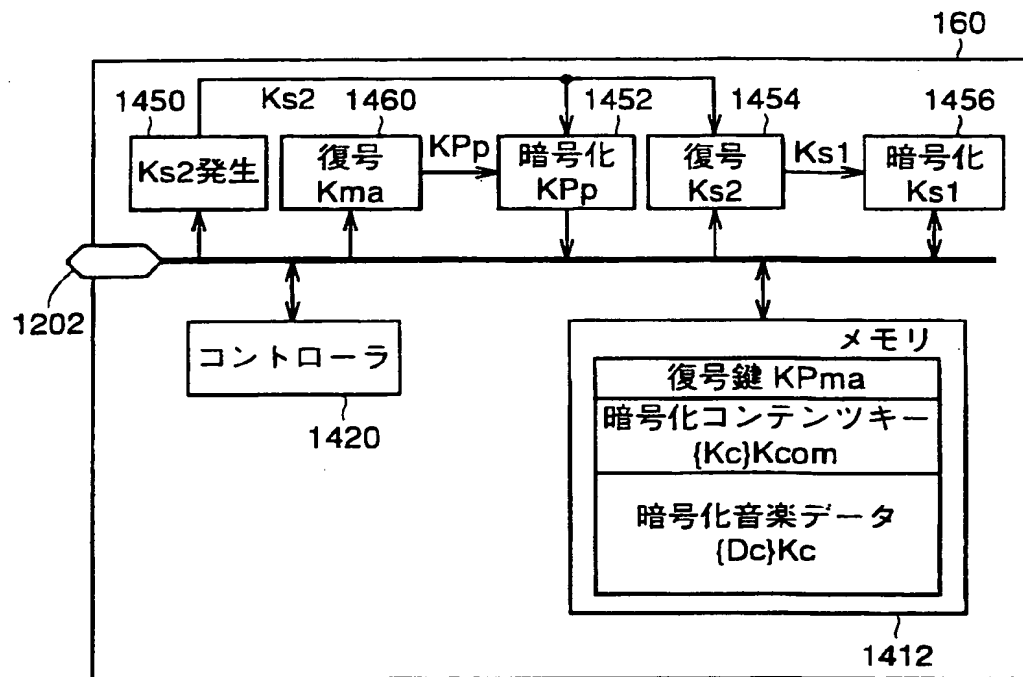
**This Page Blank (uspto)**

FIG. 20

	記号	属性	特性	
メモリカード 管理の鍵	KPma	公開復号鍵	システム共通	(KPp)KPmaの復号によってKPpの認証を行う機能を有する認証 鍵
	Ks2	共通鍵	セッションキー	メモリカードと音楽生成モジュール艦のアクセス毎に発生
音楽生成 モジュール 管理の鍵	KPp	公開暗号鍵	再生装置のクラス (種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる 非対称な秘密復号鍵Kpにて復号可能
	Kp	秘密復号鍵	再生装置のクラス (種類等)固有	データ再生装置毎或いはデータ再生装置の種類によって異なる 非対称な公開暗号鍵KPpにて暗号化した暗号データを平分化
	Kcom	秘密復号鍵	システム共通	暗号化されたコンテンツキーを復号する
	Ks1	共通鍵	セッション固有	メモリカードと音楽生成モジュール艦のアクセス毎に発生
配信データ	Kc	共通鍵	コンテンツキー	暗号化コンテンツデータの復号鍵
	Dc	データ	コンテンツデータ	例：音楽データ

**This Page Blank (uspto)**

FIG. 21



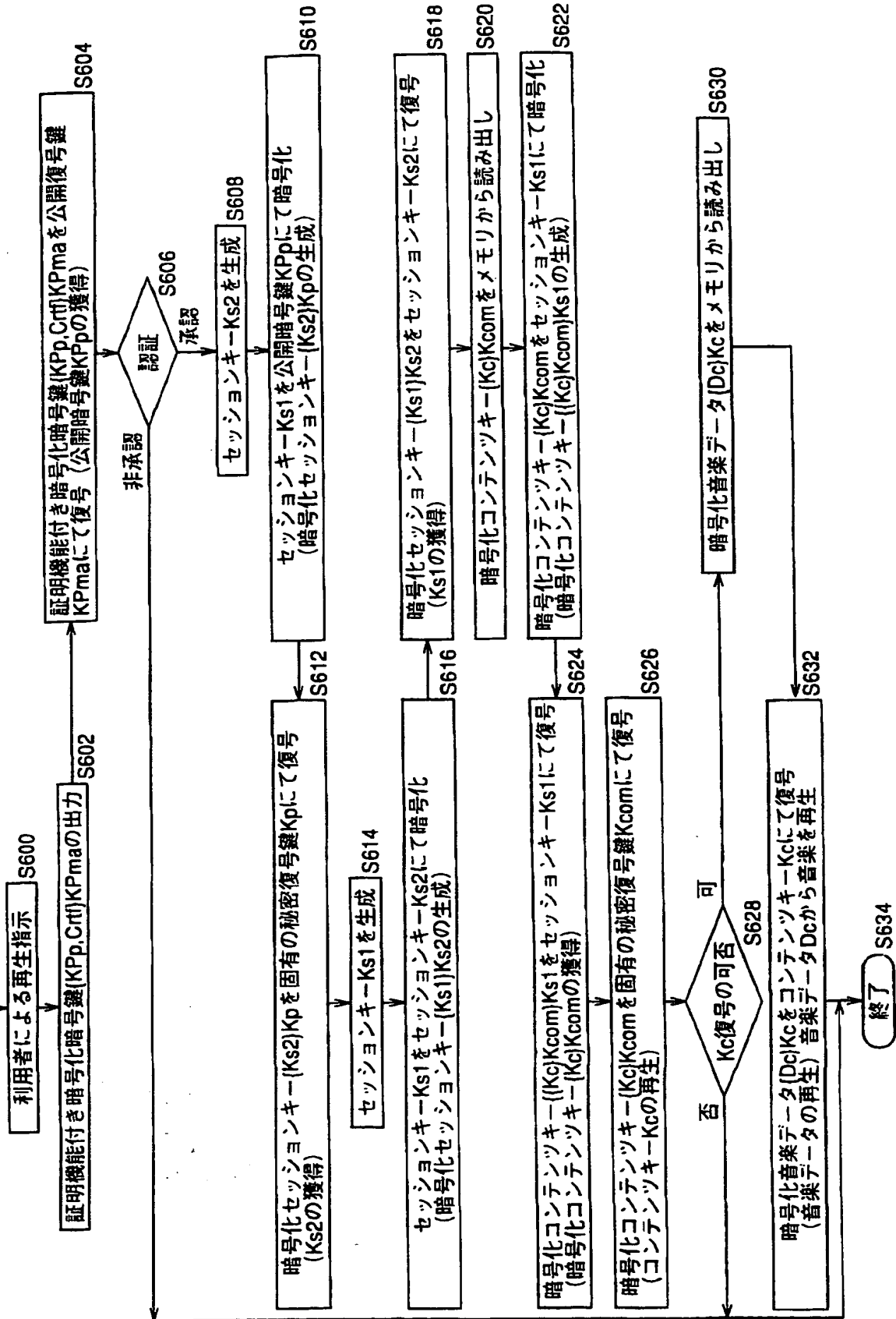
This Page Blank (uspto)



FIG. 22

本体側処理

メモリカード内処理



This Page Blank (uspto)

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05832

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G10K15/02, G06F15/00, G06F17/60, H04L9/08, H04L9/10,  
G06K19/00, H04H1/00, H04M3/42, H04M3/493, H04M11/08,  
G10L19/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G10K15/00-15/06, G10L19/00-19/14, H04L9/00-9/38,  
G09C1/00-5/00, G06F12/00, G06F12/14, H04M11/00-11/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1995 Toroku Jitsuyo Shinan Koho 1994-2000  
Kokai Jitsuyo Shinan Koho 1971-2000 Jitsuyo Shinan Toroku Koho 1996-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

INSPEC (DIALOG)  
WPI (DIALOG)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP, 817185, A2 (Kabushiki Kaisha TOSHIBA), 07 January, 1998 (07.01.98), Full text, all drawings & JP, 10-106148, A & JP, 3093678, B2 & TW, 340920, A & KR, 98086354, A & CN, 1183685, A	1 2-22
X Y	JP, 9-326166, A (Mitsubishi Electric Corporation), 16 December, 1997 (16.12.97), Full text, all drawings (Family: none)	1 2-22
Y	JP, 10-40172, A (Toshiba Corporation), 13 February, 1998 (13.02.98), Full text, all drawings (Family: none)	2-22
Y	Nikkei Electronics, No.739, "Kagata Memory Card de Ongaku Chosakuken wo mamoru", 22 March, 1999 (22.03.99), pp.49-53	2-22
Y	Nikkei Electronics, No.728, "Bei Shuuhun Kiki Maker Ootega, MP3 Keitaigata Player Hatsubai; Chosakuken taisaku ha Fuka sezu",	2-22

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:  
"A" document defining the general state of the art which is not  
considered to be of particular relevance  
"E" earlier document but published on or after the international filing  
date  
"L" document which may throw doubts on priority claim(s) or which is  
cited to establish the publication date of another citation or other  
special reason (as specified)  
"O" document referring to an oral disclosure, use, exhibition or other  
means  
"P" document published prior to the international filing date but later  
than the priority date claimed

"T" later document published after the international filing date or  
priority date and not in conflict with the application but cited to  
understand the principle or theory underlying the invention  
"X" document of particular relevance; the claimed invention cannot be  
considered novel or cannot be considered to involve an inventive  
step when the document is taken alone  
"Y" document of particular relevance; the claimed invention cannot be  
considered to involve an inventive step when the document is  
combined with one or more other such documents, such  
combination being obvious to a person skilled in the art  
"&" document member of the same patent family

Date of the actual completion of the international search  
10 November, 2000 (10.11.00)

Date of mailing of the international search report  
21 November, 2000 (21.11.00)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/JP00/05832

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	19 October, 1998 (19.10.98), pp.31-32 Nikkei Electronics, No.731, "Yogoreta Image Fusshoku Nerau MP3 Gyoukai; Ongaku Haishin no Kaigi 'Web noise' kara", 30 November, 1998 (30.11.98), pp.29-30	1-22

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int Cl' G10K15/02, G06F15/00, G06F17/60, H04L9/08, H04L9/10,  
G06K19/00, H04H1/00, H04M3/42, H04M3/493, H04M11/08,  
G10L19/00

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int Cl' G10K15/00~15/06, G10L19/00~19/14, H04L9/00~9/38,  
G09C1/00~5/00, G06F12/00, G06F12/14, H04M11/00~11/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926~1995年  
日本国公開実用新案公報 1971~2000年  
日本国登録実用新案公報 1994~2000年  
日本国実用新案登録公報 1996~2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

INSPEC (DIALOG)  
WPI (DIALOG)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	EP, 817185, A2 (Kabushiki kaisha TOSHIBA) 7.1月.1998(07.01.98), 全文全図, &JP, 10-106148, A &JP, 3093678, B2 &TW, 340920, A &KR, 98086354, A &CN, 1183685, A	1
Y		2-22
X	JP, 9-326166, A (三菱電機株式会社) 16.12月.1997(16.12.97), 全文全図, (ファミリーなし)	1
Y		2-22

☒ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

10.11.00

国際調査報告の発送日

21.11.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)  
郵便番号100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

松尾 淳一 印

5C

8842

電話番号 03-3581-1101 内線 3540

## C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P, 10-40172, A (株式会社東芝) 13.2月.1998(13.2.98), 全文全図, (ファミリーなし)	2-22
Y	日経エレクトロニクス, No.739, 「小型メモリ・カードで音楽著作権を守る」, 22.3月.1999(22.03.99), p.49-53	2-22
Y	日経エレクトロニクス, No.728, 「米周辺機器メーカー大手が, MP3携帯型プレーヤ発売 著作権対策は付加せず」, 19.10月.1998(19.10.98), p.31-32	2-22
A	日経エレクトロニクス, No.731, 「汚れたイメージ払拭ねらうMP3業界 音楽配信の会議 Webnoise から」, 30.11月.1998(30.11.98), p.29-30	1-22